KASPERSKY LAB

Kaspersky Anti-Virus® 5.0 for Windows Workstations

HANDBUCH FÜR DEN SYSTEM-ADMINISTRATOR

KASPERSKY ANTI-VIRUS® 5.0
FOR WINDOWS WORKSTATIONS

Handbuch für den Systemadministrator

© Kaspersky Lab
http://www.kaspersky.com/de

Redaktionsschluss: Juli 2006

Inhalt

KAPITEL 1. KASPERSKY ANTI-VIRUS® FOR WINDOWS WORKSTATIONS 7
1.1. Was ist neu an der Version 5.0 10
1.2. Hardware- und Softwarevoraussetzungen 12
1.3. Lieferumfang 12
1.4. Service für registrierte Benutzer 13
1.5. Bezeichnungen 14
KAPITEL 2. INSTALLATION UND DEINSTALLATION DER ANWENDUNG 15
2.1. Installation der Anwendung 15
2.2. Installation der Anwendung im silent-Modus 21
2.3. Deinstallation des Anwendung 24
2.4. Update von Version 4.x auf 5.0 25
KAPITEL 3. BEDIENUNG DES PROGRAMMS 26
3.1. Grundkonzept der Bedienung 27
3.2. Lokale Schnittstelle 28
3.2.1. Symbol in der Taskleiste 28
3.2.2. Kontextmenü 29
3.2.3. Programmhauptfenster: Allgemeine Struktur 30
3.2.3.1. Registerkarte *Sicherheit* 31
3.2.3.2. Registerkarte Einstellungen 33
3.2.3.3. Registerkarte Support 34
3.2.4. Untersuchungsfenster 36
3.2.5. Hilfesystem 37
KAPITEL 4. COMPUTERSCHUTZ OHNE ZUSATZEINSTELLUNGEN 38
4.1. Standardeinstellungen 38
4.2. Stufe der Antivirensicherheit 41
KAPITEL 5. BEDIENUNG DER ANWENDUNG ÜBER LOKALE SCHNITTSTELLE 43
5.1. Update der Antiviren-Datenbanken und der Programmmodule 43
5.1.1. Wann sollen Updates heruntergeladen werden? 44
5.1.2. Manuelles Update. Download von Updates 44
5.1.3. Update-Einstellungen 46

5.1.3.1. Update der Programmmodule ... 48
5.1.3.2. Kopieren von Updates in einen lokalen Ordner ... 50
5.1.3.3. Auswahl der Updatequelle ... 51
5.1.3.4. Konfiguration des Proxyservers ... 53
5.1.3.5. Auswahl des Typs der Antiviren-Datenbanken ... 55
5.2. Echtzeitschutz ... 56
5.2.1. Untersuchung des Dateisystems ... 59
5.2.1.1. Auswahl der Sicherheitsstufe ... 60
5.2.1.2. Auswahl der Aktion für gefundene Objekte ... 62
5.2.2. E-Mail-Untersuchung ... 64
5.2.2.1. Auswahl der Sicherheitsstufe ... 66
5.2.2.2. Auswahl der Aktion für gefundene Objekte ... 68
5.2.3. Untersuchung der E-Mails in Microsoft Office Outlook ... 69
5.2.4. Untersuchung von Makros ... 70
5.2.5. Skriptuntersuchung ... 72
5.2.6. Schutz vor Netzwerk-Angriffen ... 74
5.3. Scan auf Befehl ... 76
5.3.1. Vollständige Untersuchung des Computers ... 78
5.3.2. Untersuchung eines ausgewählten Objekts ... 79
5.3.3. Einstellungen für Scan auf Befehl ... 82
5.3.3.1. Auswahl der Untersuchungsstufe ... 85
5.3.3.2. Auswahl der Aktion für gefundene Objekte ... 88
5.3.4. Untersuchung von Archiven ... 90
5.3.5. Untersuchung von Wechseldatenträgern ... 93
5.4. Bearbeitung von gefundenen schädlichen Objekten ... 94
5.5. Aktivitätskontrolle der Programmprozesse ... 99
5.6. Benutzeraufgaben ... 101
5.7. Erstellen einer Ausnahmenliste ... 102
5.8. Konfiguration des Zeitplans ... 106
5.9. Aufgabenstart im Namen eines bestimmten Benutzers ... 110
5.10. Zusatzeinstellungen ... 111
5.10.1. Quarantäne und Backup ... 112
5.10.1.1. Einstellungen der Optionen für Quarantäne und Backup ... 112
5.10.1.2. Arbeit mit der Quarantäne ... 114
5.10.1.3. Arbeit mit Backup ... 116
5.10.2. Arbeit mit Protokollen ... 118

5.10.3. Verwaltung der Konfiguration von Kaspersky Anti-Virus 124
5.10.4. Erweiterte Einstellungen 125
5.10.5. Einstellungen für Eingabeaufforderungen 130
5.10.6. Beschränkungen der Leistung von Kaspersky Anti-Virus 131
5.10.7. Arbeit im Administrator- und Benutzermodus 131

KAPITEL 6. BEDIENUNG DER ANWENDUNG MIT KASPERSKY ADMINISTRATION KIT 133
6.1. Bedienung mit Installationspaketen 133
6.1.1. Erstellen eines Installationspakets 133
6.1.2. Anzeige und Ändern von Parametern eines Installationspakets 136
6.2. Bedienung mit Richtlinien 137
6.2.1. Anlegen einer Richtlinie 138
6.2.2. Anzeige und Bearbeitung von Richtlinien-Optionen 142
6.2.2.1. Anzeige von Informationen zur Richtlinie 143
6.2.2.2. Scan auf Befehl 144
6.2.2.3. Echtzeitschutz der Objekte des Dateisystems 147
6.2.2.4. Bedrohungen und Ausnahmen 150
6.2.2.5. Aktivitätskontrolle der Programmprozesse 151
6.2.2.6. Untersuchung von E-Mail-Nachrichten 152
6.2.2.7. Untersuchung von Skripten 155
6.2.2.8. Untersuchung von Makros 156
6.2.2.9. Schutz vor Netzwerkangriffen 159
6.2.2.10. Update der Antiviren-Datenbanken und Anwendungsmodule 160
6.2.2.11. Aktionen mit den Systemaufgaben 162
6.2.2.12. Einstellungen der Quarantäne und Backup 162
6.2.2.13. Schaffung des Protokolls über die Arbeit der Anwendung 164
6.2.2.14. Registerkarte Erweitert 167
6.2.2.15. Anzeige der Ergebnisse des Übernehmens von der Richtlinie 171
6.3. Aufgabenverwaltung 172
6.3.1. Aufgabenerstellung 172
6.3.1.1. Erstellung lokaler Aufgaben 173
6.3.1.2. Erstellung einer Gruppenaufgabe 178
6.3.1.3. Erstellung einer globalen Aufgabe 179
6.3.2. Anzeige und Korrektur der Aufgabeneinstellungen. Verfolgung der Ausführung 180
6.3.3. Starten und Beenden von Aufgaben 181

6.4. Verwaltung der Programmeinstellungen 181
6.4.1. Anzeige der Informationen über Anwendung 183
6.4.2. Zusatzeinstellungen der Anwendung 185
6.4.3. Arbeiten mit Quarantäne und Backup 186
6.4.4. Anzeige der Information über Lizenzschlüssel 188
6.4.5. Einstellungen der Optionen der Protokollerstellung 188
KAPITEL 7. TESTEN DER KORREKTEN FUNKTION VON KASPERSKY ANTI-VIRUS 190
7.1. „Testvirus“ EICAR und seine Modifikationen 190
7.2. Testen der Funktion von Kaspersky Anti-Virus 192
KAPITEL 8. VERWALTUNG DER LIZENZSCHLÜSSEL 195
8.1. Verwaltung der Lizenzschlüssel über die lokale Benutzeroberfläche: 196
8.2. Verwaltung der Lizenzschlüssel über die Schnittstelle Kaspersky Administration Kit 199
KAPITEL 9. STEUERUNG DER ANWENDUNG MIT HILFE DER BEFEHLSZEILE 200
9.1. Untersuchung ausgewählter Objekte 201
9.2. Vollständige Untersuchung 203
9.3. Updatestart 204
9.4. Rollback des letzten Updates 205
9.5. Echtzeitschutzmodus 206
9.6. Start der Anwendung 207
9.7. Beenden der Anwendung 207
9.8. Steuerung von Aufgaben 207
9.9. Import/ Export von Einstellungen 210
9.10. Hinzufügen eines Lizenzschlüssels 210
KAPITEL 10. HÄUFIGE FRAGEN 211
ANHANG A. KONTAKT ZUM TECHNISCHEN KUNDENDIENST 218
ANHANG B. GLOSSAR 221
ANHANG C. KASPERSKY LAB 229
C.1. Andere Produkte von Kaspersky Lab 230
C.2. Kontaktinformationen 239
ANHANG D. ENDBENUTZER-LIZENZVERTRAG 241

KAPITEL 1. KASPERSKY ANTI-VIRUS® FOR WINDOWS WORKSTATIONS

Kaspersky Anti-Virus® for Windows Workstations (nachfolgend auch Kaspersky Anti-Virus) dient zum Schutz für Workstations vor Viren und schädlichen Programmen.

Die Anwendung hat folgende Funktionen:

- **Schutz vor Viren und schädlichen Programmen** – Finden und Entfernen schädlicher Programme auf Ihrem Computer. Folgende zwei Basismodi der Programmfunktion, die getrennt oder gleichzeitig verwendet werden können, lassen sich unterscheiden:
    - **Echtzeitschutz für den Computer** – Virenuntersuchung aller Objekte, die auf dem Computer gestartet, geöffnet und gespeichert werden sollen.
    - **Scan auf Befehl** – Untersuchung sowohl des gesamten Computers als auch einzelner Laufwerke, Dateien oder Verzeichnisse. Sie können diese Untersuchung manuell starten oder den regelmäßigen automatischen Start der Untersuchung konfigurieren.
- **Wiederherstellung der Funktionsfähigkeit nach einem Virusangriff**. Die vollständige Untersuchung und Desinfektion mit den von Kaspersky-Lab-Experten empfohlenen Einstellungen erlaubt Ihnen, alle Viren zu finden, die Ihre Daten während eines Virusangriffs infiziert haben.
- **Untersuchung und Desinfektion eingehender/ausgehender Mail** – Virusanalyse und Desinfektion von eingehender und ausgehender Mail im Echtzeitmodus[1]. Erweiterterlaubt das Programm, die Mail-Datenbanken von Mailprogrammen auf Befehl zu untersuchen und zu desinfizieren[2].

---

[1] Es wird unabhängig von den verwendeten Mail-Protokollen der gesamte E-Mail-Verkehr untersucht, der von dem Programm Microsoft Office Outlook empfangen und gesendet wird. Außerdem werden E-Mails untersucht, die von einem beliebigen Programm nach Protokoll POP3 empfangen und nach SMTP-Protokoll gesendet werden.

[2] Kaspersky Anti-Virus bietet die Möglichkeit zur Virenuntersuchung von Mail-Datenbanken unabhängig von dem verwendeten Mailprogramm. Es werden aber nur Datenbanken für Microsoft Office Outlook und Microsoft Outlook Express desinfiziert.

- **Schutz des Computers vor Netzwerk-Angriffen** – Analyse aller Daten, die aus einem Netzwerk (lokales Netzwerk oder Internet) auf dem Benutzercomputer eingehen. Die Daten werden auf Netzwerk-Angriffe hin analysiert. Wenn ein Angriff erkannt wird, wird er abgewehrt und der angreifende Computer wird blockiert. Außerdem bietet das Programm einen Tarnmodus, in dem der Benutzercomputer nur Daten von jenen Computern annimmt, mit denen der Datenaustausch vom Benutzer initiiert wurde.

- **Update der Antiviren-Datenbanken, der Datenbanken für Netzwerk-Angriffe und der Programmmodule** – Aktualisierung der Antiviren-Datenbanken und der Datenbanken für Netzwerk-Angriffe durch Informationen über neue Viren und Angriffe, durch Desinfektionsmethoden für infizierte Objekte, sowie Update der Programmmodule (falls diese Option nicht deaktiviert wurde). Die Aktualisierung erfolgt von den Kaspersky-Lab-Updateservern, von einem benutzerdefinierten Server oder aus einem Netzwerkordner oder lokalen Ordner.

- **Empfehlungen zur Konfiguration und Arbeit des Programms** – Während der Arbeit mit Kaspersky Anti-Virus werden Tipps der Kaspersky-Lab-Experten und Empfehlungen zu den Einstellungen angezeigt, die dem optimalen Antivirenschutz entsprechen.

  Wenn gefährliche Objekte gefunden werden, wenn die Antiviren-Datenbanken längere Zeit nicht aktualisiert werden, oder der Computer längere Zeit nicht vollständig untersucht wird, können Sie im Hauptfenster von Kaspersky Anti-Virus entsprechende Tipps und Erklärungen zur Ausführung dieser Aktionen finden.

  Auf der Grundlage langjähriger Arbeitserfahrung im Bereich des Antivirenschutzes und durch die Analyse einer Vielzahl von Rückmeldungen der Anwender an den Technischen Support-Service, wurde von Kaspersky-Lab-Experten eine optimale Konfiguration des Programms ausgearbeitet. Die von Experten empfohlenen Antivirenschutzeinstellungen werden sofort nach der Installation und dem Start des Produkts wirksam.

- **Verwendung unterschiedlicher Profile für die Programmkonfiguration** – Erstellen und Übernehmen spezieller Konfigurationsdateien (*Profile)*, in denen die Parameter des Programms gespeichert sind. Die Programmparameter können in Profilen gespeichert werden, was Ihnen den einfachen Wechsel der Konfiguration von Kaspersky Anti-Virus erlaubt. Beispielsweise können Sie das Programm speziell für die Arbeit im Echtzeitschutz-Modus oder für die Ausführung des Scan auf Befehl konfigurieren, und solche Konfigurationen bei Bedarf verwenden. Während der Arbeit mit Kaspersky Anti-Virus können Sie jederzeit zu den empfohlenen Programmeinstellungen zurückkehren.

- **Verwendung von zwei Modi für die Programmarbeit**: Option zur Arbeit mit dem Programm im *Benutzermodus* oder im *Administratormodus*. Im Benutzermodus steht nur die Grundfunktionalität von Kaspersky Anti-Virus zur Verfügung, es ist aber nicht möglich, die Anwendungseinstellungen zu ändern und den Antivirenschutz abzuschalten. Im Administratormodus ist die vollständige Steuerung der Anwendung möglich.

- **Verschieben von Objekten in die Quarantäne** – Verschieben von Objekten, die möglicherweise von Viren oder Virusmodifikationen infiziert sind, in einem speziellen und sicheren Speicher, in dem Sie die Objekte desinfizieren, löschen, im Ausgangsordner wiederherstellen, und zur Analyse an die Experten von Kaspersky Lab senden können. Die Quarantänedateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

- **Anlegen von Sicherungskopien der Objekte** – Anfertigen von Sicherungskopien in einem speziellen Backup-Speicher vor der Desinfektion oder dem Löschen von Objekten. Solche Kopien werden zur eventuell erforderlichen Wiederherstellung des Originalobjekts angefertigt, wenn es sich um wertvolle Daten handelt, oder zum Zweck der Wiederherstellung eines Infektionsbildes. Die Kopien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

- **Protokollführung** – Aufzeichnung aller Arbeitsergebnisse von Kaspersky Anti-Virus in einem Protokoll. Das Detailprotokoll über die Untersuchungsergebnisse enthält eine Gesamtstatistik der untersuchten Objekte. Außerdem werden Informationen über die Einstellungen, mit denen eine bestimmte Aufgabe ausgeführt wurde, und die Untersuchungs- und Bearbeitungsreihenfolge jedes einzelnen Objekts gespeichert. Auch über die Ergebnisse der Updates und über die Ergebnisse des Echtzeitschutzes wird ein Protokoll geführt.

- **Zentrale Fernsteuerung der Antivirensicherheit**: Verwaltung der Anwendung mit Hilfe des Systems zur zentralisierten Administration Kaspersky Administration Kit 5.0.

Bestimmte Funktionen von Kaspersky Anti-Virus sind bei der Arbeit mit Hilfe der Befehlszeile verfügbar (Details s. Kapitel 9 auf S. 200).

1.1. Was ist neu an der Version 5.0

Die Version 5.0 von **Kaspersky Anti-Virus for Windows Workstations** unterscheidet sich in folgenden Punkten von der Vorgängerversion 4.x:

- *Verwendung der Beschleunigungstechnologien* iChecker und iStreams *für die Antivirenuntersuchung*. Kaspersky Anti-Virus untersucht nun Objekte, die während einer vorhergehenden Untersuchung gescannt wurden und sich seitdem nicht geändert haben, nicht erneut. Dies gilt sowohl für den Echtzeitschutz als auch für den Scan auf Befehl. Dadurch erhöht sich die Operationsgeschwindigkeit des Programms wesentlich.
- *Untersuchung und Desinfektion von E-Mails*, die mit einem beliebigen Mailprogramm nach POP3-Protokoll empfangen und nach SMTP-Protokoll gesendet werden. Die Vorgängerversion bot den E-Mail-Antivirenschutz lediglich für Microsoft Office Outlook.
- *Desinfektion infizierter Archive.* Kaspersky Anti-Virus erlaubt die Desinfektion infizierter Dateien in Archiven der Typen *zip*, *arj*, *cab*, *rar*, *lha* und *ice*. In der Vorgängerversion des Programms waren nur das Erkennen infizierter Dateien in Archiven und die Desinfektion infizierter Objekte in zip-Archiven möglich.

  Multi-Level-Archive der genannten Formate und selbstextrahierende Archive werden von Kaspersky Anti-Virus untersucht, aber nicht desinfiziert.
- *Die Geschwindigkeit des Updates der Antiviren-Datenbanken* wurde durch Definition des geografisch nächstliegenden Kaspersky-Lab-Updateservers erhöht. Nach einer Verbindungsunterbrechung muss nur noch der verbleibende Teil eines Updates heruntergeladen werden.
- *Schutz vor Netzwerk-Angriffen*. Diese Version von Kaspersky Anti-Virus schützt Ihren Computer vor den momentan am meisten verbreiteten Netzwerk- und Hacker-Angriffen.
- *Einfaches Interface*. Das Produkt besteht aus einem Programm, während die vorhergehende Version aus mehreren Programmen bestand, von denen jedes eine spezielle Funktion des Antivirenschutzes erfüllte. Die neue Konzeption erlaubt einfachen Zugriff und Verwaltung aller wichtigen Funktionen von Kaspersky Anti-Virus.
- *Die Kompatibilität von Kaspersky Anti-Virus mit anderen Antivirenprodukten wurde verbessert*. Bei der Programminstallation können Sie den Schutz für das Dateisystem, für E-Mails, für Netzwerke und die Untersuchung ausführbarer Skripts ablehnen, wenn dieser Schutz durch andere Anwendungen auf Ihrem Computer gewährleistet wird.

- *Empfohlene Einstellungen und Experten-Tipps*. Zur Vereinfachung der Arbeit mit dem Programm gelten in dieser Produktversion Standardeinstellungen, die von Kaspersky-Lab-Experten empfohlen werden. In den meisten Fällen ist vor der Verwendung des Programms keine Konfiguration erforderlich. Wenn sich der Antivirenschutz auf einem niedrigen Niveau befindet, gibt das Programm eine entsprechende Meldung aus und schlägt unterschiedliche Varianten zur Optimierung des Sicherheitsniveaus vor.

- *Verwaltung von Profilen für die Arbeit mit dem Programm*. Die Programmeinstellungen können zur späteren Verwendung in einer speziellen Datei gespeichert werden. Wenn die empfohlenen Einstellungen von Kaspersky Anti-Virus nicht für Sie geeignet sind, können Sie diese entsprechend anpassen und die Konfiguration in einem *Profil* speichern.

- *Verlängerung der Lizenz für die Produktbenutzung*. Kaspersky Anti-Virus Version 5.0 erlaubt Ihnen die Installation eines Lizenzschlüssels zur Verlängerung der Lizenz für die Produktbenutzung.

- *Senden von Objekten zur Expertise an Kaspersky Lab.* Sie können jetzt möglicherweise infizierte Objekte, die von Kaspersky Anti-Virus gefunden werden, sowie Dateien, die Sie persönlich für infiziert halten, zur Analyse an Kaspersky Lab senden.

- *Verbot des Löschens von infizierten Mail-Datenbanken.* Infizierte Mail-Datenbanken werden nicht mehr mit Hilfe von Kaspersky Anti-Virus gelöscht. Allerdings können Sie diese Objekte wie früher manuell entfernen.

- *Option zum Erstellen einer Liste der vertrauenswürdigen Programmprozesse*. Die Dateiaktivität der vertrauenswürdigen Prozesse wird von Kaspersky Anti-Virus im Echtzeitschutz nicht kontrolliert.

- *Kennwortschutz für den Zugriff auf die Einstellungen* von Kaspersky Anti-Virus. Sie können ein Kennwort festlegen, das beim Wechsel zwischen Benutzer- und Administratormodus abgefragt wird. Im Benutzermodus kann nicht auf die Programmeinstellungen zugegriffen werden, der Echtzeitschutz kann nicht deaktiviert und Kaspersky Anti-Virus kann nicht aus dem Arbeitsspeicher entfernt werden.

1.2. Hardware- und Softwarevoraussetzungen

Damit das Kaspersky Anti-Virus for Windows Workstations optimal funktioniert, muss die Workstation folgende Voraussetzungen erfüllen:

Generelle Voraussetzungen:

- 50 MB freier Festplattenspeicher
- CD-ROM-Laufwerk (für die Installation von Kaspersky Anti-Virus von CD-ROM)
- Microsoft Internet Explorer Version 5.5 und höher (für das Update der Antiviren-Datenbanken und Programmmodule über das Internet).

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Prozessor Intel Pentium 300 MHz oder mehr
- 64 MB freier Arbeitsspeicher

Microsoft Windows 2000 Professional (Service Pack 2 oder höher), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 oder höher):

- Prozessor Intel Pentium 300 MHz oder mehr
- 128 MB freier Arbeitsspeicher

1.3. Lieferumfang

Die Software kann bei unseren Vertriebspartnern (als verpackte Variante) oder in einem Online-Shop (z. B. www.kaspersky.com/de, Abschnitt **E-STORE**) erworben werden.

Wenn Sie die Software als verpackte Variante erwerben, umfasst der Lieferumfang die folgenden Komponenten:

- Versiegelter Umschlag mit Installations-CD, die Programmdateien enthält.
- Benutzerhandbuch;
- Lizenzschlüssel, der zu einem Distributionspaket gehört oder auf einem speziellen Datenträger gespeichert ist;
- Lizenzvertrag.

Bitte lesen Sie vor dem Öffnen des versiegelten Umschlags mit der Installations-CD sorgfältig den Lizenzvertrag.

Beim Erwerb von Kaspersky Anti-Virus for Workstations in einem Online-Shop kopieren Sie das Produkt von der Kaspersky-Lab-Internetseite. Die Distribution enthält neben dem eigentlichen Produkt auch die vorliegende Dokumentation. Der Lizenzschlüssel befindet sich in der Verpackung oder wird Ihnen nach Eingang der Bezahlung per E-Mail zugesandt.

Der Lizenzvertrag ist eine rechtsgültige Vereinbarung zwischen Ihnen und Kaspersky Lab, in der festgelegt wird, zu welchen Bedingungen Sie das von Ihnen erworbene Softwareprodukt verwenden dürfen.

Bitte lesen Sie den Lizenzvertrag sorgfältig durch!

Wenn Sie den Bedingungen des Lizenzvertrags nicht zustimmen, können Sie die Packung mit Kaspersky Anti-Virus an den Händler zurückgeben, bei dem Sie sie erworben haben. Der Kaufbetrag des Abonnements wird dann an Sie zurückerstattet. Voraussetzung dafür ist, dass der versiegelte Umschlag mit der Installations-CD nicht geöffnet wurde.

Durch das Öffnen der versiegelten Verpackung mit der Installations-CD oder die Installation der Software auf dem Computer stimmen Sie allen Bedingungen des Lizenzvertrags zu!

1.4. Service für registrierte Benutzer

Kaspersky Lab bietet legalen Benutzern ein breites Spektrum an Serviceleistungen, die eine gesteigerte Effektivität von Kaspersky Anti-Virus ermöglichen.

Durch den Erwerb eines Abonnements werden Sie zum registrierten Programmbenutzer und können während der Gültigkeitsdauer Ihres Abonnements folgende Serviceleistungen in Anspruch nehmen:

- Nutzung neuer Versionen des betreffenden Softwareprodukts;
- Beratung in Fragen zu Installation, Konfiguration und Benutzung des betreffenden Softwareprodukts per Telefon oder E-Mail
- Nachrichten über das Erscheinen neuer Softwareprodukte von Kaspersky Lab und über das Auftauchen neuer Viren (Dieser Service gilt für Benutzer, die den Newsletter von Kaspersky Lab abonniert haben).

Wir können keine Beratung zur Funktionsweise und zum Einsatz von Betriebssystemen sowie zu Funktionen anderer Technologien geben.

1.5. Bezeichnungen

Der Text dieses Handbuchs wird sinngemäß durch verschiedene Layout-Elemente hervorgehoben. In der Tabelle unten finden Sie die verwendeten Bezeichnungen.

Gestaltung	Sachliche Übereinstimmung
Fettschrift	Namen von Menüs, Menüpunkten, Fenstern, Elementen aus Dialogfeldern u. ä.
Anmerkung.	Zusatzinformationen, Anmerkungen
Achtung!	Informationen, die besonders zu beachten sind
Um eine Aktion auszuführen 1. Schritt 1. 2. …	Beschreibung einer Abfolge vom Benutzer auszuführender Schritte und möglicher Aktionen
Aufgabe, Beispiel	Aufgabenstellung, Beispiel, um die Möglichkeiten der Software darzustellen

KAPITEL 2. INSTALLATION UND DEINSTALLATION DER ANWENDUNG

Es gibt zwei Installationsmöglichkeiten für Kaspersky Anti-Virus 5.0 for Windows Workstations: Lokale und Ferninstallation (mit dem Fernverwaltungssystem Kaspersky Administration Kit). In diesem Benutzerhandbuch wird die lokale Installation von Kaspersky Anti-Virus beschrieben. Nähere Angaben über die Ferninstallation der Anwendung finden Sie im Hilfesystem für Kaspersky Administration Kit 5.0.

2.1. Installation der Anwendung

Es wird empfohlen, vor Installation von Kaspersky Anti-Virus alle auf dem Computer laufenden Anwendungen zu beenden.

Um die Anwendung zu installieren, starten Sie die ausführbare Datei, die zur Distribution gehört.

Die Installation der Anwendung von einer Distribution, die aus dem Internet heruntergeladen wurde, stimmt vollständig mit der Installation der Anwendung von der Distributions-CD überein.

Das Setup funktioniert im Dialogmodus. Jedes Fenster enthält eine bestimmte Auswahl von Schaltflächen zur Steuerung des Installationsprozesses. Unten finden Sie die Funktionsbeschreibung der wichtigsten Schaltflächen:

- **Weiter >** – Aktion bestätigen und zum nächsten Schritt des Installationsvorgangs übergehen.
- **< Zurück** – zum vorhergehenden Installationsschritt zurückkehren.
- **Abbrechen** – die Installation des Produkts abbrechen.
- **Fertig stellen** – den Vorgang zur Installation des Programms auf dem Computer fertig stellen.

Betrachten wir die einzelnen Schritte der Installationsprozedur ausführlich.

Schritt 1. Überprüfung der Version des installierten Betriebssystems

Vor der Programminstallation wird auf Ihrem Computer die Übereinstimmung von installiertem Betriebssystem und Service Packs mit den Installationsvoraussetzungen für Kaspersky Anti-Virus überprüft.

Sollten bestimmte Voraussetzungen nicht erfüllt sein, dann erscheint eine entsprechende Meldung auf dem Bildschirm. Es wird empfohlen, die erforderlichen Programme und Service Packs mit Hilfe des Diensts **Windows Update** (oder auf andere Weise) zu installieren, bevor mit der Installation von Kaspersky Anti-Virus begonnen wird.

Schritt 2. Startfenster des Installationsvorgangs

Nach dem Start der ausführbaren Datei auf dem Bildschirm das Startfenster geöffnet, das Informationen über den Beginn der Installation von Kaspersky Anti-Virus auf Ihrem Computer enthält.

Klicken Sie auf **Weiter >**, um die Installation fortzusetzen. Die Installation des Produkts kann durch Klick auf **Abbrechen** abgebrochen werden.

Schritt 3. Lesen der Lizenzvereinbarung

Das Dialogfenster **Lizenzvereinbarung** enthält den Text der Lizenzvereinbarung. Bitte lesen Sie diese aufmerksam. Wenn Sie allen Punkten der Vereinbarung zustimmen, klicken Sie auf **Akzeptieren**. Klicken Sie auf die Schaltfläche **Abbrechen**, um die Programminstallation abzulehnen.

Schritt 4. Angabe von Benutzerinformationen

Geben Sie im Dialogfenster **Benutzerinformationen** die erforderlichen Informationen ein. Füllen Sie die Felder **Benutzername** und **Firma** aus. Diese Felder enthalten standardmäßig die Daten aus der Microsoft Windows-Registrierung.

Schritt 5. Lesen wichtiger Informationen über das Programm

Auf dieser Installationsetappe erhalten Sie wichtige Informationen über das Programm. In diesem Fenster werden die wichtigsten Optionen, funktionelle Besonderheiten usw. von Kaspersky Anti-Virus genannt.

Um zum nächsten Installationsschritt überzugehen, klicken Sie auf die Schaltfläche **Weiter >**.

Schritt 6. Verwendung von Kaspersky-Lab-Technologien

Bei diesem Schritt der Installation von Kaspersky Anti-Virus können Sie entscheiden, ob bei der Arbeit von Kaspersky Anti-Virus folgende Technologien verwendet werden:

Echtzeitschutz des Dateisystems – Virenuntersuchung aller Dateien, die auf dem Computer gestartet, geöffnet und gespeichert werden sollen. Der Dateischutz ist standardmäßig aktiviert. Wenn Sie nicht möchten, dass Kaspersky Anti-Virus Dateien beim Zugriff untersucht, entfernen Sie das Kontrollkästchen ☑ **Dateisystem-Echtzeitschutz verwenden**.

Echtzeitschutz für E-Mails – Virenuntersuchung aller auf Ihrem Computer eintreffenden und von Ihnen abgesendeten E-Mails, sowie Ihrer Mail-Datenbanken. Der Mail-Schutz ist standardmäßig aktiviert. Damit Kaspersky Anti-Virus E-Mails nicht auf Viren untersucht, deaktivieren Sie das Kontrollkästchen ☑ **E-Mail-Echtzeitschutz verwenden**.

Untersuchung der Skriptausführung – Virenanalyse aller Java-Skripts, die in beim Öffnen von Internetseiten in Microsoft Internet Explorer geöffnet werden sollen. Die Skriptuntersuchung ist standardmäßig aktiviert. Wenn Sie möchten, dass Kaspersky Anti-Virus keine Skriptuntersuchung durchführt, deaktivieren Sie das Kontrollkästchen ☑ **Skriptuntersuchung verwenden**.

Makrountersuchung – Untersuchung aller VBA-Makros, die auf dem Computer gestartet werden sollen, auf das Vorhandensein von schädlichem Code. Die Makrountersuchung ist standardmäßig aktiviert. Um die Makrountersuchung abzuschalten, deaktivieren Sie das Kontrollkästchen ☑ **Makrountersuchung verwenden**.

Echtzeitschutz vor Netzwerk-Angriffen – Technologie zum Schutz Ihres Computers vor Hackerangriffen. Diese Technologie verhindert Angriffe aus einem Netzwerk auf Ihren Computer und schützt Ihre Daten vor Beschädigung, unerwünschtem Zugriff und Diebstahl. Der Netzwerk-Echtzeitschutz ist standardmäßig deaktiviert. Um den Schutz zu verwenden, aktivieren Sie das Kontrollkästchen **Netzwerk-Echtzeitschutz verwenden**.

iStreams™–Technologie – Technologie zur Beschleunigung der Antivirenuntersuchung von Objekten (Eine ausführliche Beschreibung der Technologie befindet sich in Anhang B auf S. 221). Um die Verwendung der Technologie abzuschalten, deaktivieren Sie das Kontrollkästchen **iStreams™-Technologie verwenden**.

Diese Technologie wird nur auf Sektoren mit NTFS-Dateisystem verwendet.

Wenn Sie die Verwendung der oben genannten Technologien auf dieser Etappe ablehnen, ist für ihre spätere Installation der erneute Start der Produktinstallation und die Auswahl der gewünschten Technologien erforderlich.

Wenn Sie sich bei der Arbeit mit Kaspersky Anti-Virus entscheiden, eine bestimmte Art des Echtzeitschutzes oder die Streams™-Technologie nicht mehr zu verwenden, muss die Programminstallation erneut gestartet und bei diesem Schritt das entsprechende Kontrollkästchen deaktiviert werden.

Klicken Sie auf die Schaltfläche **Weiter >**, um die Installation fortzusetzen.

Schritt 7. Suche nach anderen Antivirenprogrammen

Auf dieser Etappe erfolgt die Suche nach anderen installierten Antivirenprodukten einschließlich Kaspersky-Lab-Produkten, deren gemeinsame Verwendung mit Kaspersky Anti-Virus bei der Arbeit der Anwendung zu Konflikten führen kann.

Beim Fund einer auf Ihrem Computer installierten älteren Version von Kaspersky Anti-Virus (z.B. Version 4.5) wird die Anwendung automatisch von Version 4.x auf Version 5.0 aktualisiert (Details s. Pkt. 2.4 auf S. 25).

Wenn ein Lizenzschlüssel für Kaspersky Anti-Virus for Windows Workstations Version 4.x gefunden wird, dann werden während des Installationsprozesses im Fenster zur Installation des Lizenzschlüssels (s. Schritt 8. auf S. 19) Informationen darüber angezeigt. Für die Arbeit der Anwendung können Sie diesen Lizenzschlüssel verwenden oder einen anderen wählen.

Beim Fund von auf Ihrem Computer installierter Antivirensoftware eines anderen Herstellers erscheint auf dem Bildschirm ein Dialogfenster mit einer Liste der Anwendungen, die entfernt werden sollen, bevor Kaspersky Anti-Virus installiert wird.

Wir empfehlen Ihnen, das betreffende Programm zu entfernen. Klicken Sie dazu auf **Nein**, um den Installationsvorgang abzubrechen. Entfernen Sie dann das betreffende Softwareprodukt und starten Sie die ausführbare Datei erneut.

Die Kaspersky-Lab-Spezialisten warnen davor, mehrere Antiviren-produkte auf einem Computer zu installieren, weil bei der gleichzeitigen Arbeit Konflikte entstehen können.

Wenn erkannt wird, dass Kaspersky Anti-Virus 5.0 for Windows Workstations bereits auf Ihrem Computer installiert ist, wird die früher installierte Version durch diese Programmkopie aktualisiert.

Bei der Aktualisierung von Version 5.0 enthält das Fenster zur Installation des Lizenzschlüssels (s. Schritt 8. auf S. 19) keine Informationen über den Schlüssel, der zuvor installierte Schlüssel wird aber für die Arbeit der Anwendung verwendet.

Schritt 8. Installation des Lizenzschlüssels

Im Dialogfenster **Lizenzschlüssel** wird der Lizenzschlüssel gewählt, auf dessen Basis Kaspersky Anti-Virus das Vorhandensein einer Lizenzvereinbarung überprüft und deren Gültigkeitsdauer ermittelt.

Der Lizenzschlüssel ist Ihr persönlicher "Schlüssel". Er enthält Dienstinformationen, die für die volle Funktionsfähigkeit des Programms notwendig sind. Dazu zählen:

- Informationen zur technischen Unterstützung (Supportanbieter und deren Adressen).
- Bezeichnung, Nummer und Gültigkeitsdauer der Lizenz.

Um einen neuen Lizenzschlüssel zu installieren,

1. Klicken Sie auf die Schaltfläche **Durchsuchen** und gehen Sie im Standardauswahlfenster zu dem Ordner, der die Lizenzschlüsseldatei enthält:

   - Wenn Sie Kaspersky Anti-Virus in einer Packung erworben haben, ist der Lizenzschlüssel auf einer Diskette gespeichert. Legen Sie die Diskette in das Laufwerk ein und wechseln Sie zu dieser Diskette.
   - Wenn die Lizenz in einem Internetshop gekauft wurde, speichern Sie den per E-Mail erhaltenen Lizenzschlüssel in einem Ordner auf der Festplatte Ihres Computers und wechseln Sie zu diesem Ordner.

   Im gewählten Ordner wird einen Liste der verfügbaren Lizenzschlüssel angezeigt.

2. Wählen Sie den gewünschten Lizenzschlüssel (Datei mit der Erweiterung **.key**) und klicken Sie auf die Schaltfläche **Öffnen**.

Dadurch werden im Fenster des Installationsassistenten Informationen über die Lizenz und den Pfad der Lizenzschlüsseldatei angezeigt.

Klicken Sie auf die Schaltfläche **Weiter >**, um die Installation des Programms fortzusetzen.

Sollten Sie im Moment der Programminstallation nicht über einen Lizenzschlüssel verfügen (z.B. wenn Sie diesen bei Kaspersky Lab über das Internet bestellt, aber noch nicht erhalten haben), dann können Sie den Schlüssel später, beim Start des Programms oder mit Hilfe des speziellen Hilfsprogramms zur Lizenzschlüsselinstallation (s. Kapitel 8 auf S. 195) installieren. Beachten Sie, dass Sie ohne Schlüssel nicht mit der Arbeit von Kaspersky Anti-Virus beginnen können.

Schritt 9. Auswahl des Installationsordners

Im Dialogfenster **Auswahl des Installationsordners** wird der Ordner festgelegt, in den Kaspersky Anti-Virus installiert werden soll. Die Auswahl des Ordners erfolgt mit Hilfe der Schaltfläche **Durchsuchen**.

Mit Hilfe der Schaltfläche **Wiederherstellen** kann der Pfad des Installationsordners wiederhergestellt werden, der standardmäßig von der Anwendung angeboten wird: **<Laufwerk>\Programme\Kaspersky Lab\Kaspersky Anti-Virus 5.0 for Windows Workstations**.

Im Fenster, das durch Klick auf **Laufwerk** geöffnet wird, werden Informationen über den vorhandenen und für die Installation erforderlichen Platz auf den logischen Laufwerken der Workstation angezeigt.

Klicken Sie auf die Schaltfläche **Installieren**, um die Installation fortzusetzen. Danach wird das Kopieren der Dateien von Kaspersky Anti-Virus gestartet.

Schritt 10. Fertigstellen der Installationsprozedur

Das Fenster **Abschluss des Installationsassistenten** enthält Informationen über das Fertigstellen des Installationsvorgangs von Kaspersky Anti-Virus auf Ihrem Computer.

Um die Programminstallation fertig zu stellen, müssen bestimmte Dienste im System registriert werden. Deshalb wird Ihnen der Neustart des Computers angeboten. Dies ist zum korrekten Abschluss der Produktinstallation NOTWENDIG. Klicken Sie im folgenden Fenster auf die Schaltfläche **Ja**, um den Neustart sofort vorzunehmen, oder auf **Nein**, um den Computer später neu zu starten.

Nach der Installation von Kaspersky Anti-Virus:

- erscheint das Programmsymbol im Infobereich der Taskleiste.
- werden Verknüpfungen mit dem Programm zum Windows-Hauptmenü hinzugefügt (**Start → Programme → Kaspersky Anti-Virus 5.0 for Windows Workstations**).

2.2. Installation der Anwendung im silent-Modus

Kaspersky Anti-Virus 5.0 for Windows Workstations kann aus der Befehlszeile installiert werden. Wechseln Sie dazu in den Ordner, in dem sich die Distribution der Anwendung befindet, und verwenden Sie den Befehl:

```
setup [/s] [/l<Protokolldatei>]
[/p<Eigenschaften>="<Wert>"…][3]
```

Schlüssel	Funktion
/s	Verwendung des Modus zur silent-Installation.
/l<Protokolldatei>	Ausgabe von Ereignissen in die angegebene **Protokolldatei**. Die Pfadangabe der Datei kann absolut oder relativ sein. Der Pfad wird in Anführungszeichen angegeben, wenn er ein Leerzeichen enthält.
/p<Eigenschaften>	Angabe der Parameter für die Installation der Anwendung. Folgende Parameter stehen zur Verfügung: • **INSTALLDIR** – vollständiger Pfad des Ordners für die Installation der Anwendung • **USERNAME** – Benutzername • **COMPANYNAME** – Name der Firma des Benutzers • **KLKEY** – vollständiger Pfad der Schlüsseldatei • **KLUSEIDS** – Dieser Parameter steuert die Verwendung des Schutzes vor Netzwerkangriffen. Um die Technologie zu verwenden, wählen Sie den Wert **"1"**, um die Technologie zu deaktivieren den Wert **""**. Die Verwendung dieser Technologie ist standardmäßig

[3] Optionale Schlüssel werden in eckigen Klammern angegeben.

Schlüssel	Funktion
	deaktiviert. • **KLUSEISTREAMS** – Dieser Parameter steuert die Verwendung der Technologie iStreams™. Um die Technologie zu verwenden, wählen Sie den Wert **"1"**, um die Technologie zu deaktivieren, den Wert **""**. Die Verwendung dieser Technologie ist standardmäßig aktiviert. • **KLUNINSTPASSWD** – Kennwort, das bei der Deinstallation der Anwendung abgefragt wird. • **KLADMPASSWD** – Kennwort für den Wechsel aus dem Benutzermodus in den Administrator-modus. • **KLDELAYREBOOT** – Dieser Parameter legt fest, ob der Computer nach dem Abschluss der Installation neu gestartet werden soll. Um den Neustart festzulegen, wählen Sie den Wert **"1"**, um ihn zu deaktivieren, den Wert **""**. Der Neustart ist standardmäßig aktiviert. • **KLUSERTPFILE** – Dieser Parameter steuert die Verwendung des Echtzeitschutzes für Dateien. Um die Technologie zu verwenden, wählen Sie den Wert **"1"**, um die Technologie zu deaktivieren, den Wert **""**. Die Verwendung dieser Technologie ist standardmäßig aktiviert. • **KLUSERTPMAIL** – Dieser Parameter steuert die Verwendung des E-Mail-Echtzeitschutzes. Um die Technologie zu verwenden, wählen Sie den Wert **"1"**, um die Technologie zu deaktivieren, den Wert **""**. Die Verwendung dieser Technologie ist standardmäßig aktiviert. • **KLUSERTPSCRIPT** – Dieser Parameter steuert die Verwendung der Untersuchung von zu startenden Skripts. Um die Technologie zu verwenden, wählen Sie den Wert **"1"**, um die Technologie zu deaktivieren, den Wert **""**. Die Verwendung dieser Technologie ist standard-mäßig aktiviert. • **KLUSERTPMACRO** – Dieser Parameter steuert die Verwendung der Makrounter-

Schlüssel	Funktion
	suchung. Um die Technologie zu verwenden, wählen Sie den Wert **"1"**, um die Technologie zu deaktivieren, den Wert **""**. Die Verwendung dieser Technologie ist standardmäßig aktiviert.

Beispiel:

```
setup /s /l"C:/Kaspersky Lab/Report"
/pINSTALLDIR="C:/Kaspersky Lab" /pKLADMPASSWD=password
```

Die Parameter für die Installation im silent-Modus können auch in der ini-Datei im Abschnitt **[Setup]** festgelegt werden.

Die Datei mit den Parametern muss den Namen **setup.ini** tragen.

Folgende Parameter werden verwendet:

- **InstallDir** – vollständiger Pfad des Ordners zur Installation der Anwendung
- **User** – Benutzername
- **Company** – Name der Firma des Benutzers
- **Key** – vollständiger Pfad der Lizenzschlüsseldatei
- **IDS** – Verwendung der Technologie zum Schutz vor Netzwerkangriffen (Werte: **enable** – aktiviert, **disable** – deaktiviert).
- **IStreams** – Verwendung der Technologie iStreams™ (Werte: **enable** – aktiviert, **disable** – deaktiviert).
- **UninstallPassword** – Kennwort, das bei der Deinstallation der Anwendung abgefragt wird.
- **AdminPassword** – Kennwort für den Wechsel vom Benutzermodus in den Administratormodus.
- **Reboot** – Neustart des Computers nach der Installation der Anwendung (Werte: **yes** – aktiviert, **no** – deaktiviert).
- **RTPFile** – Verwendung der Technologie zum Echtzeitschutz von Dateien (Werte: **enable** – aktiviert, **disable** – deaktiviert).
- **RTPMail** – Verwendung der Technologie zum Echtzeitschutz der E-Mail (Werte: **enable** – aktiviert, **disable** – deaktiviert).

- **RTPScript** – Verwendung der Technologie zur Untersuchung von ausführbaren Skripts (Werte: **enable** – aktiviert, **disable** – deaktiviert).
- **RTPMacro** – Verwendung der Technologie zur Makrountersuchung (Werte: **enable** – aktiviert, **disable** – deaktiviert).

Beispiel:

```
[Setup]
InstallDir=C:/Kaspersky Lab
Key=A:/License/00000001.key
User=Ivanov
IStreams=enable
```

2.3. Deinstallation des Anwendung

Wenn Sie aus irgendwelchen Gründen **Kaspersky Anti-Virus** deinstallieren möchten, gehen Sie auf **Start → Programme → Kaspersky Anti-Virus for Windows Workstations/Deinstallation von Kaspersky Anti-Virus** oder verwenden Sie das Microsoft Windows-Standardmittel **Programme ändern und entfernen**.

Wenn das Programm vom Kaspersky Administration Kit verwaltet wird und ein Kennwortschutz für die nicht sanktionierte Deinstallation aktiviert wurde (s. Pkt. 6.2.2.14 auf S. 167), wird zu Beginn der Deinstallation dieses Kennwort abgefragt.

Sie werden dann in einem Dialogfeld gebeten, die Deinstallation zu bestätigen. Um die Deinstallationsroutine zu starten, klicken Sie auf die Schaltfläche **OK**. Danach erscheint ein Fenster, in dem Sie wählen können, Objekte zu löschen oder zu speichern, die sich in der Quarantäne und im Backup befinden. Das gleiche trifft für die Protokolldateien und Lizenzschlüssel zu.

Der Deinstallationsvorgang startet und alle Dateien der Anwendung werden von der Festplatte des Computers gelöscht.

Wenn beim Deinstallieren des Programms eine Datei gefunden wird, die von anderen Anwendungen verwendet werden kann, erscheint ein Dialogfeld zur Bestätigung des Löschens der Datei. Um eine Datei zu löschen, klicken Sie auf **Ja**.

Im Anschluss an die Deinstallation der Anwendung erscheint ein Dialogfeld und fordert Sie auf, die Workstation neu zu starten. Wählen Sie die gewünschte Variante aus und klicken Sie auf **Fertig stellen**.

2.4. Update von Version 4.x auf 5.0

Vor dem Start des Updates von Kaspersky Anti-Virus wird empfohlen, die Objekte zu bearbeiten, die sich im Quarantäne- und Backup-Speicher befinden.

Zum Update von Kaspersky Anti-Virus for Windows Workstations von Version 4.x auf 5.0 starten Sie die ausführbare Datei. Während der Installation wird die ältere Version von Kaspersky Anti-Virus entfernt.

Zum Abschluss der Installation ist der Neustart des Betriebssystems erforderlich.

Bitte beachten Sie, dass beim Update von Kaspersky Anti-Virus die Einstellungen von Version 4.x erhalten bleiben. Sie können die empfohlenen Einstellungen verwenden, die standardmäßig gelten, oder die Anwendung selbst konfigurieren.

Bei entfernter Programminstallation über Kaspersky Administration Kit (Details s. Hilfesystem für Kaspersky Administration Kit 5.0) erfolgt das Update von Version 4.x auf 5.0 automatisch: Dabei wird die ältere Version von Kaspersky Anti-Virus entfernt und der entfernte Computer wird neu gestartet.

KAPITEL 3. BEDIENUNG DES PROGRAMMS

Kaspersky Anti-Virus 5.0 for Windows Workstations wird auf einer Workstation installiert und kann auf einem Computer lokal oder entfernt mit dem Modul Kaspersky Administration Kit (falls der Computer an ein zentrales Fernverwaltungssystem angeschlossen ist) verwaltet werden.

Es gibt einige Benutzer-Kategorien, die mit Kaspersky Anti-Virus arbeiten können:

- *Workstationbenutzer* – Person, auf deren Computer Kaspersky Anti-Virus installiert ist.
- *Administrator für die Antivirus-Sicherheit* (im Weiteren – Administrator) – Person, die Kaspersky Anti-Virus lokal bedient.
- *Administrator des logischen Netzes* – Person, die Kaspersky Anti-Virus über das zentrale Fernverwaltungssystem Kaspersky Administration Kit bedient.

Je nach den Rechten verfügt jede Benutzerkategorie über eine Schnittstelle, die dem Benutzer die ihm zustehenden Programmfunktionen bereitstellt:

Die Benutzer-Schnittstelle wurde für den effizienten Einsatz von MS Office optimiert. Damit können folgende Aufgaben erledigt werden:

- Ansicht von Statusinformationen über den Zustand der Antivirus-Sicherheit;
- Starten von Untersuchungsaufgaben für Objekte im Dateisystem;
- Aktualisierung der Antiviren-Datenbanken und Anwendungsmodule (wenn diese Option vom Administrator aktiviert wurde);
- Ansicht von Statusinformationen über den Zustand des Antivirenschutzes;
- Ansicht der Ergebnisse der Aufgabenausführung und des Ereignisjournals;
- Anzeige des Inhalts der Quarantäne- und Backup-Ablagen, Senden von Quarantäne-Dateien zur Analyse an Kaspersky Lab.

Die erweiterte **Schnittstelle für Administratoren** erlaubt neben den Benutzeraufgaben die schnelle und flexible Konfiguration der Arbeit von Kaspersky Anti-Virus. Außerdem stehen folgende Aufgaben zur Verfügung:

- Einstellung der Aufgaben des Echtzeit-Antivirenschutzes;
- Erstellen von Aufgaben zur Untersuchung von Objekten im Dateisystem und Aktualisierungsaufgaben, deren Bedienung und Planung sowie deren Start nach Zeitplan;

Bei zentralisierter Steuerung mit dem Kaspersky Administration Kit wird der Computer von einem Fernrechner aus verwaltet, auf dem die *Administrationskonsole* installiert ist.

Die Administrationskonsole ist eine standardmäßige **Schnittstelle, die in MMC integriert ist** und mit welcher der Administrator die folgenden Aufgaben erledigen kann:

- Entfernte Installation von Kaspersky Anti-Virus auf Client-Computern;
- Update der Antiviren-Datenbanken und der Anwendungsmodule;
- Verwaltung von Richtlinien und Aufgaben auf Clients;
- Aktivierung von Lizenzschlüsseln auf Clients;
- Ansicht der Programmprotokolle auf Clients;

Um die Anwendung über Kaspersky Administration Kit zu verwalten, muss auf dem Client-Computer der Administrationsagent installiert sein, der die Kommunikation zwischen Workstation und Administrationsserver gewährleistet (Details s. Hilfesystem zu KASPERSKY ADMINISTRATION KIT 5.0).

Näheres zum Konzept der zentralisierten Steuerung finden Sie im Handbuch für den Administrator „Kaspersky Administration Kit 5.0“.

3.1. Grundkonzept der Bedienung

Bei lokalem Betrieb von Kaspersky Anti-Virus bestimmt der Administrator die Programmeinstellungen und die Anpassung der Aufträge.

Aufgabe – Bezeichnung für eine von Kaspersky Anti-Virus auszuführende Aktion. Je nach den Funktionen werden Aufträge nach Typen (vollständige Untersuchung, Update der Antiviren-Datenbanken und der Programmmodule usw.) unterschieden. Jeder konkreten Aufgabe entspricht eine Auswahl von Parametern für die Ausführung während der Arbeit der Anwendung. Dies sind die *Einstellungen der Aufgabe*.

Programmeinstellungen – Satz von zusätzlichen Einstellungen des Programms, zu denen Optionen für die Quarantäne, das Backup und für den Service für den Erhalt von Protokollen usw. zählen.

Bei zentralisierter Steuerung über Kaspersky Administration Kit bestimmt der Administrator die Einstellungen für die Aufgaben und die Einstellungen für die Anwendung, die auf entfernten Netzwerkcomputern installiert ist.

Die Besonderheit einer zentralisierten Steuerung besteht darin, dass Remote-Rechner in Gruppen organisiert werden können und deren Einstellungen über die Anlage und Zuweisung von Gruppenrichtlinien bedient werden.

Richtlinie – Programmoptionen in der Gruppe des logischen Netzwerkes und Ausnahmen für diese Optionen bei Konfiguration des Programms oder einer Aufgabe.

Zur Richtlinie gehören die Optionen für eine vollständige Konfiguration aller Programmfunktionen. So gehören zur Richtlinie auch die Programmkonfiguration und die Einrichtung von allen Auftragstypen, jedoch sind die Optionen ausgenommen, die unmittelbar beim Start des Auftrags bestimmt werden müssen.

3.2. Lokale Schnittstelle

Kaspersky Anti-Virus hat eine einfache und bequeme Schnittstelle. In diesem Kapitel werden die Grundelemente behandelt: das Symbol in der Taskleiste, das Kontextmenü, das Hauptfenster und einige Servicefenster.

3.2.1. Symbol in der Taskleiste

Nach dem Programmstart erscheint im Infobereich der Taskleiste ein Symbol, dessen Aussehen vom Zustand des Antivirenschutzes abhängt (ob der Echtzeitschutz aktiviert ist und der Scan auf Befehl gestartet wurde):

Wenn das Symbol aktiv ist (rote Farbe) , befinden sich alle Dateien auf Ihrem Computer unter der Kontrolle von Kaspersky Anti-Virus. Wenn das Symbol inaktiv ist (graue Farbe) , ist der Echtzeitschutz abgeschaltet (beispielsweise wenn Sie den Echtzeitschutz zuvor angehalten, den Echtzeitschutz für Dateien deaktiviert oder seine Verwendung bei der Installation abgelehnt haben).

Wenn die vollständige Untersuchung des Computers, die Untersuchung einer einzelnen Datei oder Laufwerks oder die Echtzeitschutzanalyse eines Objekts ausgeführt wird, dann wird in der Taskleiste ein blinkendes Symbol angezeigt . Während der Untersuchung von E-Mails erscheint das Symbol . Während des Updates der Antiviren-Datenbanken, der Netzwerk-Angriffsdatenbanken und der Anwendungsmodule nimmt das Symbol folgendes Aussehen an: .

Wenn in den erweiterten Einstellungen für Kaspersky Anti-Virus (s. Pkt. 5.10.4 auf S. 125) die Animation des Symbols im Infobereich deaktiviert wurde, nimmt das Symbol nur einen Zustand an: aktiv oder inaktiv.

Beim Eintritt eines Ereignisses, das in Bezug auf die Antivirensicherheit wichtig ist, wird über dem Symbol vorübergehend eine Meldung mit Empfehlungen der Kaspersky-Lab-Experten eingeblendet (Bei der Arbeit mit den Betriebssystemen Microsoft Windows 98/NT werden diese Hinweise nicht angezeigt).

3.2.2. Kontextmenü

Wenn Sie mit der rechten Maustaste in der Taskleiste das Programmsymbol anklicken, öffnet sich das Kontextmenü (s. Abbildung 1), das folgende Punkte enthält:

- **Kaspersky Anti-Virus öffnen** – Das Hauptfenster auf der Registerkarte **Sicherheit** öffnen. Diesen Vorgang können Sie duplizieren, indem Sie mit der linken Maustaste auf das Programmsymbol in der Taskleiste klicken.
- **In den Benutzermodus wechseln / In den Administratormodus wechseln** – Von einem Sicherheitsmodus in den anderen wechseln.
- **Gestartete Aufgaben** – Liste der Aufgaben, die nach Zeitplan ausgeführt werden. Dieser Punkt erscheint im Kontextmenü, wenn eine Aufgabe ausgeführt wird.
- **Arbeitsplatz auf Viren untersuchen** – Start der umfassenden Virensuche im Computer entsprechend der gewählten Sicherheitsstufe.
- **Datenbanken updaten** – Update der Antiviren-Datenbanken starten.
- **Echtzeitschutz aktivieren / Echtzeitschutz anhalten** – Den Echtzeitschutz Ihres Computers aktivieren bzw. vorübergehend deaktivieren. Dieser Punkt ist nur dann im Kontextmenü des Programms vorhanden, wenn Sie die Verwendung des Datei-Echtzeitschutzes bei der Installation von Kaspersky Anti-Virus for Windows Workstations nicht abgelehnt haben. Abhängig vom Echtzeitschutz-Status ändert sich das Aussehen des Programmsymbols. Abhängig davon, ob der Echtzeitschutz aktiviert ist oder nicht, ändert sich das Aussehen des Programmsymbols. Dieser Punkt steht nur dem Administrator von Kaspersky Anti-Virus zur Verfügung, der normale Benutzer kann den Echtzeitschutz des Rechners nicht aktivieren/deaktivieren.

Wir warnen davor, den Echtzeitschutz zu beenden, weil sich dadurch das Risiko einer Infektion Ihres Computers durch Viren wesentlich erhöht.

- **Über das Programm** – Öffnen eines Fensters mit der Information über Kaspersky Anti-Virus 5.0 for Windows Workstations.
- **Beenden** – Kaspersky Anti-Virus aus dem Arbeitsspeicher Ihres Computers entfernen. Dieser Menüpunkt steht nur dem Administrator von Kaspersky Anti-Virus zur Verfügung.

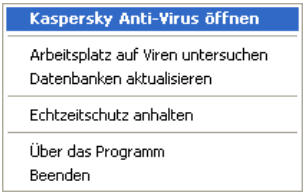

Abbildung 1. Kontextmenü

3.2.3. Programmhauptfenster: Allgemeine Struktur

Das Hauptfenster von Kaspersky Anti-Virus dient der Realisierung aller Optionen der Anwendung, um einen umfassenden Antivirenschutzes für Ihren Computer zu gewährleisten. Sie können folgende Aktionen ausführen:

- Starten und Beenden der Untersuchung des Computers und einzelner Laufwerke, Ordner und Dateien des Computers auf das Vorhandensein von Viren und anderen schädlichen Programmen.
- Erstellen von benutzerdefinierten Aufgaben zur Objektuntersuchung.
- Download der Updates für die Antiviren-Datenbanken, die Datenbanken für Netzwerk-Angriffe und die Programmmodule.
- Anpassen der Parameter für den Antivirenschutz.
- Arbeit mit den Objekten in der Quarantäne.
- Arbeit mit den Kopien, die von Objekten vor der Desinfektion oder dem Löschen im Backup-Speicher angelegt werden.
- Arbeit mit Protokollen.
- Verwaltung der Programmkonfiguration usw.

Alle Einstellungen des Antivirenschutzes, erforderliche Informationen und Aufgaben sind auf folgenden Registerkarten des Hauptfensters angeordnet:

- **Sicherheit** – Status und Aufgaben des Antivirenschutzes (Untersuchung von Objekten und Update der Antiviren-Datenbanken). Von dieser Registerkarte können Sie zur Arbeit mit Quarantäne, Backup und Protokollen wechseln. Sie wird beim Öffnen des Programms stets zuerst geöffnet (s. Pkt. 3.2.3.1 auf S. 31).
- **Einstellungen** – Status und Aufgaben zur Konfiguration der wichtigsten Antivirenschutzeinstellungen (s. Pkt. 3.2.3.2 auf S. 33).
- **Support –** Auf dieser Registerkarte erhalten Sie Informationen über den Lizenzschlüssel, können die Lizenz für die Nutzung des Programms verlängern, das Hilfesystem öffnen und Anfragen an den Technischen Support-Service senden (s. Pkt. 3.2.3.3 auf S. 34).

Jede Registerkarte besteht aus zwei Teilen:

- Die *linke Seite der Registerkarte* enthält die Hyperlinks, mit denen bei der Arbeit von Kaspersky Anti-Virus die Antivirenschutzaufgaben ausgeführt werden können. Die Liste der Aufgaben ist von der Funktion der Registerkarte abhängig. Die Registerkarte **Sicherheit** enthält beispielsweise die Aufgaben für die Virenuntersuchung Ihres Computers, die Registerkarte **Einstellungen** enthält die Einstellungen dieser Aufgaben, und die Registerkarte **Support** die Aufgaben, die der Unterstützung Ihres Antivirenschutzes dienen.
- Die *rechte Seite der Registerkarte* enthält Informationen über den aktuellen Zustand des Antivirenschutzes Ihres Computers (Echtzeitschutz, Scan auf Befehl und Antiviren-Datenbanken). Auf der Registerkarte **Sicherheit** wird der Status des Antivirenschutzes dargestellt, auf der Registerkarte **Einstellungen** der Status der Antivirenschutzeinstellungen, und auf der Registerkarte **Support** der Status der Lizenz (Informationen zum Lizenzschlüssel), Links zu den Supportadressen, Informationen über das Programm und Ihr System.

3.2.3.1. Registerkarte *Sicherheit*

Die Registerkarte **Sicherheit** (s. Abbildung 2) dient dem Start von Aufgaben zur Untersuchung Ihres gesamten Computers oder einzelner Laufwerke, Ordner und Dateien. Hier können Sie außerdem:

- die Aktualisierung der Antiviren-Datenbanken, Programmmodule und Datenbanken der bekannten Netzwerk-Angriffe starten.
- zur Arbeit mit Protokollen über die Ausführung aller gestarteten Aufgaben wechseln (anzeigen, löschen, in Datei exportieren).

- zur Arbeit mit Objekten wechseln, die möglicherweise von Viren oder deren Modifikationen infiziert sind und in der Quarantäne gespeichert wurden.
- zur Arbeit mit den Sicherheitskopien desinfizierter oder gelöschter Objekte wechseln.

Die Aufgaben können durch die entsprechenden Hyperlinks gestartet werden.

Kaspersky Anti-Virus fur Windows Workstations
Kaspersky Anti-Virus
for Windows Workstations
Sicherheit
Einstellungen
Support
Arbeitsplatz untersuchen
Kritische Bereiche untersuchen
Objekte untersuchen
Updatedownload
Quarantäne
Backup
Protokolle
Der Echtzeitschutz ist nicht vollständig aktiviert.
Die Aufgabe Schutz vor Netzwerk-Angriffen ist nicht installiert.
Die empfohlene Sicherheitsstufe wurde gewählt.
Die vollständige Untersuchung von Arbeitsplatz wurde nicht ausgeführt.
Das Ausführen der vollständigen Untersuchung des Computers ist sofort erforderlich.
Die zeitgesteuerte Untersuchung des Computers ist aktiviert. Nächster Start: morgen, 20:00.
Die Antiviren-Datenbanken sind aktuell.
Die von Ihnen verwendeten Antiviren-Datenbanken sind von heute (20-04-2006 12:28:55). Automatisches Update der Datenbanken ist aktiviert.
Nächstes Update: heute, 21:40.
Während der aktuellen Sitzung wurden keine gefährlichen Objekte gefunden.
Es wurden untersucht: 2434 Dateien und 2 Skript(s).
Kaspersky Lab, 1996-2006. Alle Rechte vorbehalten.
KASPERSKY lab

Abbildung 2. Registerkarte **Sicherheit**

Auf der rechten Seite der Registerkarte wird der *aktuelle Status des Echtzeitschutzes*, *der vollständigen Untersuchung des Computers* und *der Antiviren-Datenbanken* angezeigt. Abbildung 2 zeigt ein Beispiel, in dem der Echtzeitschutz des Computers deaktiviert ist und die vollständige Untersuchung des Computers gerade ausgeführt wurde. Außerdem befinden sich hier Kommentare zum Zustand jeder Antivirenschutzaufgabe.

Der kritische und der von den empfohlenen Einstellungen abweichende Status enthalten jeweils *Empfehlungen der Kaspersky-Lab-Experten*. Es kann sein, dass Ihnen zur Steigerung des Antivirenschutzes vorgeschlagen wird, die aktuellen Einstellungen zu ändern, zu den von Experten empfohlenen Einstellungen zurückzukehren, eine Aufgabe zu starten usw. Alle Empfehlungen enthalten Links, mit deren Hilfe die entsprechenden Aktionen ausgeführt werden können.

Wenn während der Untersuchung infizierte oder verdächtige Objekte gefunden wurden, werden auf der rechten Seite der Registerkarte entsprechende Informationen angezeigt. Mit Hilfe des Hyperlinks diese Objekte zu bearbeiten können Sie später jederzeit zur Bearbeitung der gefundenen Objekte übergehen (Details s. Pkt. 5.4 auf S. 94).

3.2.3.2. Registerkarte Einstellungen

Die Registerkarte **Einstellungen** (s. Abbildung 3) erlaubt Ihnen, den Status der Einstellungen zu beurteilen und die grundlegenden und erweiterten Einstellungen für die Arbeit von Kaspersky Anti-Virus anzupassen.

Die rechte Seite der Registerkarte zeigt den aktuellen Zustand der Einstellungen für Echtzeitschutz, vollständige Untersuchung des Computers auf Befehl und automatisches Update der Antiviren-Datenbanken, Programmmodule und Netzwerksangriffsdatenbanken mit detaillierten Kommentaren. Außerdem befinden sich hier Tipps zum Ändern bestimmter Einstellungen. Wenn Sie die Aktualisierung der Antiviren-Datenbanken beispielsweise manuell gestartet haben, dann empfiehlt das Programm Ihnen, den Downloadprozess für Updates durch die Konfiguration eines Zeitplans für diese Aufgabe zu automatisieren.

Mit Hilfe der Hyperlinks auf der linken Seite der Registerkarte können Sie zur Auswahl und Änderung der Einstellungen für den Echtzeitschutz Ihres Computers, Scans auf Befehl und Update wechseln. Außerdem kann eine Liste der vom Schutz auszuschließenden Objekte angelegt und der Typ der zu verwendenden Antiviren-Datenbanken festgelegt werden.

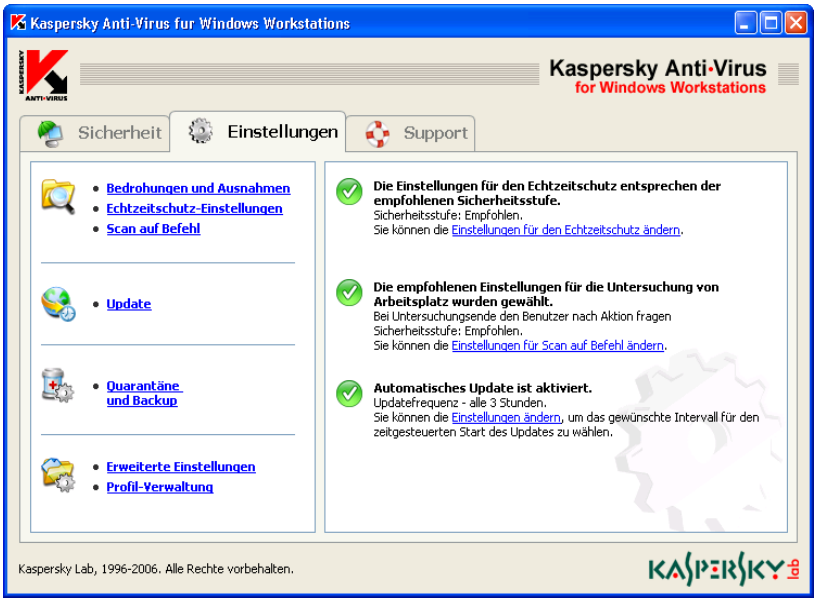
Kaspersky Anti-Virus für Windows Workstations
Kaspersky Anti-Virus
for Windows Workstations
Sicherheit
Einstellungen
Support
Bedrohungen und Ausnahmen
Echtzeitschutz-Einstellungen
Scan auf Befehl
Update
Quarantäne und Backup
Erweiterte Einstellungen
Profil-Verwaltung
Die Einstellungen für den Echtzeitschutz entsprechen der empfohlenen Sicherheitsstufe.
Sicherheitsstufe: Empfohlen.
Sie können die Einstellungen für den Echtzeitschutz ändern.
Die empfohlenen Einstellungen für die Untersuchung von Arbeitsplatz wurden gewählt.
Bei Untersuchungsende den Benutzer nach Aktion fragen
Sicherheitsstufe: Empfohlen.
Sie können die Einstellungen für Scan auf Befehl ändern.
Automatisches Update ist aktiviert.
Updatefrequenz - alle 3 Stunden.
Sie können die Einstellungen ändern, um das gewünschte Intervall für den zeitgesteuerten Start des Updates zu wählen.
Kaspersky Lab, 1996-2006. Alle Rechte vorbehalten.
KASPERSKY lab

Abbildung 3. Registerkarte **Einstellungen**

Hier können Sie auch die Einstellungen der Quarantäne anpassen, in der Objekte gespeichert werden, die möglicherweise von Viren oder Virusmodifikationen infiziert sind. Außerdem kann hier der Backup-Speicher konfiguriert werden, der zum Speichern der Sicherheitskopien von Objekten dient. Zur Konfiguration der erweiterten Einstellungen von Kaspersky Anti-Virus gelangen Sie auch über den Hyperlink Erweiterte Einstellungen.

Kaspersky Anti-Virus bietet Ihnen die Möglichkeit, unterschiedliche Konfigurationen für die Arbeit von Anti-Virus zu erstellen und diese in speziellen Dateien (*Profilen*) zu speichern. Später können Sie bequem zu einer bestimmten Konfiguration zurückkehren, ohne das Programm erneut anzupassen. Es ist ausreichend, das gewünschte Profil zu laden. Mit Hilfe des Hyperlinks Profil-Verwaltung gelangen Sie in das Fenster zum Erstellen und Laden von Profilen.

3.2.3.3. Registerkarte Support

Auf der Registerkarte **Support** (s. Abbildung 4) befinden sich Informationen darüber, an wen Sie sich wenden können, wenn bei der Arbeit mit Kaspersky Anti-Virus Probleme oder Situationen eintreten, die Sie nicht selbständig lösen können. Außerdem befinden sich hier Informationen zum Programm, zum Lizenzschlüssel und zum Betriebssystem Ihres Computers, die Sie bei Bedarf

dem Technischen Support-Service von Kaspersky Lab mitteilen können. Alle genannten Informationen befinden sich auf der rechten Seite der Registerkarte.

Die linke Seite der Registerkarte enthält Hyperlinks mit folgenden Funktionen:

- Senden von Anfragen an den Technischen Support-Service und von Objekten, die möglicherweise von Viren oder Virusmodifikationen infiziert sind, zur Analyse an Kaspersky Lab.
- Verlängerung der Lizenz für die Benutzung von Kaspersky Anti-Virus.

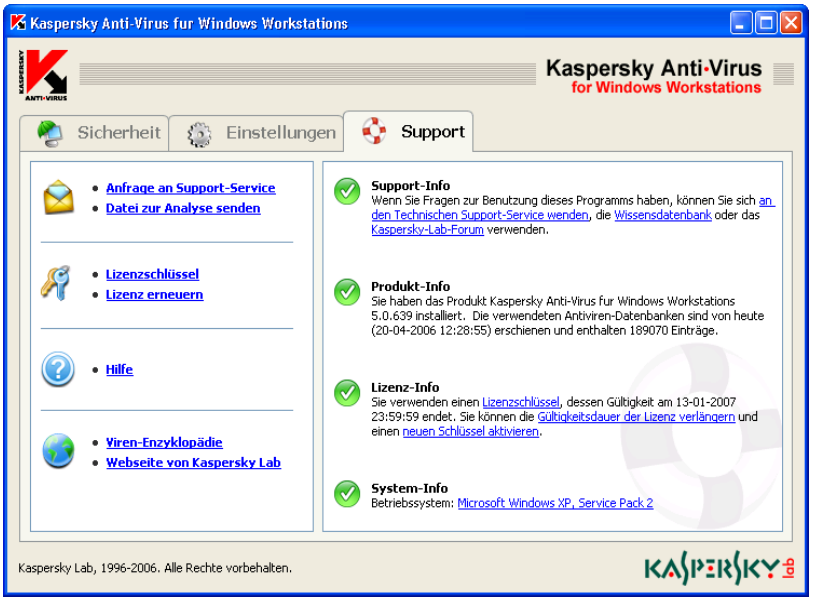
Kaspersky Anti-Virus fur Windows Workstations
Kaspersky Anti-Virus
for Windows Workstations
Sicherheit
Einstellungen
Support
Anfrage an Support-Service
Datei zur Analyse senden
Lizenzschlüssel
Lizenz erneuern
Hilfe
Viren-Enzyklopädie
Webseite von Kaspersky Lab
Support-Info
Wenn Sie Fragen zur Benutzung dieses Programms haben, können Sie sich an den Technischen Support-Service wenden, die Wissensdatenbank oder das Kaspersky-Lab-Forum verwenden.
Produkt-Info
Sie haben das Produkt Kaspersky Anti-Virus fur Windows Workstations 5.0.639 installiert. Die verwendeten Antiviren-Datenbanken sind von heute (20-04-2006 12:28:55) erschienen und enthalten 189070 Einträge.
Lizenz-Info
Sie verwenden einen Lizenzschlüssel, dessen Gültigkeit am 13-01-2007 23:59:59 endet. Sie können die Gültigkeitsdauer der Lizenz verlängern und einen neuen Schlüssel aktivieren.
System-Info
Betriebssystem: Microsoft Windows XP, Service Pack 2
Kaspersky Lab, 1996-2006. Alle Rechte vorbehalten.

Abbildung 4. Registerkarte **Support**

Auf der linken Seite der Registerkarte befinden sich außerdem Links zu Hilfeinformationen:

- Hilfe – Hilfesystem für das Produkt.
- Virus-Enzyklopädie – Link zu der Seite www.viruslist.com, die eine detaillierte Beschreibung aller im Moment existierenden schädlichen Programme enthält.
- Webseite von Kaspersky Lab – Link auf die Homepage von Kaspersky Lab.

3.2.4. Untersuchungsfenster

Wird die Untersuchung des Computers oder einzelner Objekte (Datenträger, Ordner, Dateien) gestartet, erscheint auf dem Bildschirm das Untersuchungsfenster (s. Abbildung 5).

Das Fenster besteht aus zwei Teilen:

- Der obere Bereich enthält einen Indikator, der mit Prozentangabe über die Ausführung des Untersuchungsprozesses informiert. Außerdem werden hier der Name des momentan untersuchten Objekts, die voraussichtliche Abschlusszeit der Untersuchung und eine Statistik über die Anzahl der bisher untersuchten, desinfizierten, gelöschten und in die Quarantäne verschobenen Objekte angezeigt.

- Der untere Teil des Fensters wird durch die Schaltfläche geöffnet. Er besteht aus drei Registerkarten: **Protokoll** – mit einem Bericht über die bei der Untersuchung eingetretenen Ereignisse, **Statistik** – mit den Untersuchungsergebnissen, und **Einstellungen** – mit einer Liste der Einstellungen, die bei der Untersuchung verwendet werden. Der untere Teil kann durch die Schaltfläche ausgeblendet werden.

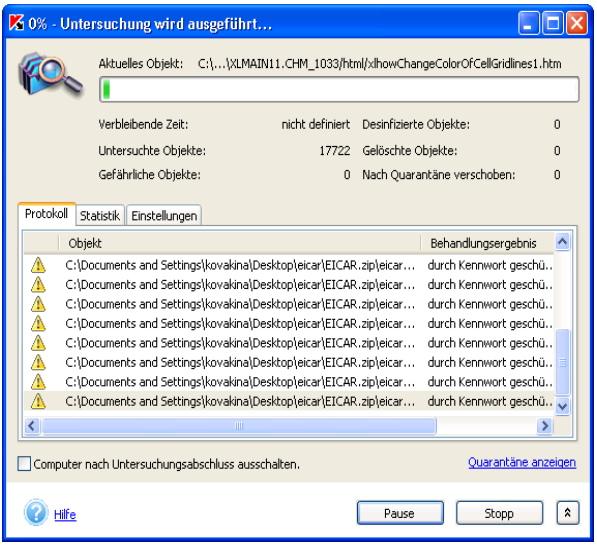

Abbildung 5. Untersuchungsfenster

Mit dem Hyperlink Quarantäne anzeigen können Sie in das Fenster des Quarantänespeichers wechseln (s. Punkt 5.10.1.2 auf S. 114).

Wenn Sie die vollständige Untersuchung des Computers ausführen, können Sie in diesem Fenster einen Modus festlegen, in dem der Computer nach dem Abschluss der Untersuchung ausgeschaltet wird. Dieser Modus kann beispielsweise verwendet werden, wenn Sie die Antivirenuntersuchung des Computers kurz vor Feierabend starten und nicht auf deren Ende warten möchten.

Um diesen Modus zu verwenden, sind allerdings folgende Vorkehrungen zu treffen: Vor dem Start der Untersuchung muss die Kennwortabfrage bei der Objektuntersuchung deaktiviert werden (s. Pkt. 5.3.3.1 auf S. 85), falls diese aktiviert war, und der Modus zur automatischen Bearbeitung von gefährlichen Objekten, deren Löschen / Verschieben in die Quarantäne, oder das Protokollieren von Informationen (s. Pkt. 5.3.3.2 auf S. 88) festgelegt werden. Dadurch wird der interaktive Programmmodus abgeschaltet und der Untersuchungsprozess wird nicht unterbrochen (während der Untersuchung erfolgen keine Eingabeaufforderungen).

Damit der Computer nach dem Abschluss der Untersuchung abgeschaltet wird, aktivieren Sie das Kontrollkästchen **Computer nach Untersuchungsabschluss ausschalten**.

3.2.5. Hilfesystem

Von der Registerkarte **Support** aus besteht Zugriff auf das vollständige Hilfesystem für das Programm. Zum Öffnen des Hilfesystems dient der Hyperlink Hilfe auf der linken Seite der Registerkarte.

Sollte eine Frage zu einem bestimmten Dialogfenster auftreten, dann drücken Sie die Funktionstaste **<F1>** oder verwenden Sie den Hyperlink Hilfe in der unteren linken Ecke des betreffenden Fensters.

KAPITEL 4. COMPUTERSCHUTZ OHNE ZUSATZEINSTELLUNGEN

Der Antivirenschutz wird nach der Installation der Anwendung auf dem Computer sofort wirksam und wendet dafür Standardeinstellungen an. Diese Einstellungen sind von den Experten des Kaspersky Lab für den optimalen Schutz ihres Rechners empfohlen.

Bei zentralisierter Verwaltung mit Kaspersky Administration Kit können die Einstellungen mit vom Sicherheitsadministrator erstellten Richtlinien und Aufgaben festgelegt werden. Dazu muss für die betreffenden Parameter das "Schloss" geschlossen sein. Details s. Hilfesystem für Kaspersky Administration Kit 5.0.

Außerdem ist die Möglichkeit der schnellen Änderung von Einstellungen mittels drei von Experten des Kaspersky Lab entwickelten Schutzstufen verwirklicht: *Maximale Sicherheit, Empfohlen, Maximales Tempo.*

4.1. Standardeinstellungen

Die Standardeinstellungen gelten für jede Antivirenschutz-Aufgabe:

ECHTZEITSCHUTZ IM MONITORING-MODUS

Der Echtzeitschutz Ihres Computers wird nur dann gewährleistet, wenn Sie bei der Programminstallation seine Verwendung nicht abgelehnt haben.

Bei standardmäßigem Echtzeitschutz wird das empfohlene Niveau mit folgenden Einstellungen verwendet:

- Analysiert werden Dateien, für die Lese- und Schreibberechtigung vorliegen und die sich ausführen lassen, darunter:
    - Dateien auf Festplatten und Wechseldatenträgern, Bootsektoren;
    - Dateien auf Netzdatenträgern;
    - Gepackte Dateien, OLE-Objekte und zusätzliche NTFS-Streams;

- iChecker™ und iStreams™ werden genutzt;
- Beim Fund eines infizierten Objektes unternimmt Kaspersky Anti-Virus einen Reparaturversuch. Soweit die Reparatur nicht in Frage kommt, wird das Objekt gelöscht und dabei eine Kopie im Backup angelegt. Wird ein verdächtiges Objekt erkannt, wird es in die Quarantäne verschoben.
- Beim Fund eines potentiell gefährlichen Programms erlaubt oder blockiert die Kaspersky Anti-Virus dessen Ausführung und protokolliert entsprechende Informationen.
- Der E-Mail-Verkehr wird untersucht:
    - Die Untersuchung der mit dem POP3-Protokoll eingehenden Nachrichten und die Untersuchung von Archivdateien sind aktiviert.
    - Die Untersuchung der mit dem SMTP-Protokoll ausgehenden Nachrichten ist deaktiviert.
- Die von Anwendungen des Microsoft Office verwendeten VBA-Makrobefehle werden untersucht. Sollte ein verdächtiger Makrobefehl erkannt werden, wird von Kaspersky Anti-Virus dessen Ausführung gesperrt.
- Die dynamischen Skripte von VBScript und JavaScript werden untersucht, die vom Microsoft Internet Explorer oder dem betriebssystemseitigen Skript-Bearbeitungsmodul verarbeitet werden. Sollte ein verdächtiges Skript festgestellt werden, blockiert das Kaspersky Anti-Virus dessen Ausführung.
- Der Schutz vor Netzwerk-Angriffen ist deaktiviert.

SCAN AUF BEFEHL

Für eine vollständige Antiviren-Untersuchung wird standardmäßig das *empfohlene Niveau* mit folgenden Einstellungen verwendet:

- Eine vollständige Untersuchung erfolgt nach Zeitplan jeden Freitag um 20.00 Uhr.
- Analysiert werden:
    - Dateien auf Festplatten und Wechseldatenträgern, Bootsektoren;
    - Dateien, die sich in den Ressourcen des Arbeitsspeichers befinden sowie Objekte im Autostart (Startup-Objekte), zusätzliche NTFS-Streams;
    - Eingepackte Dateien, Archive, selbst entpackende Archive, OLE-Objekte;

Bei der vollständigen Untersuchung des Computers werden die verwendeten Mailboxen nicht untersucht.

- iChecker™ und iStreams™ werden verwendet;
- Nicht untersucht werden Objekte in Netzlaufwerken, in Mail-Datenbanken sowie E-Mail-Dateien im Textformat.
- Beim Fund eines infizierten oder verdächtigen Objekts, verzögert Kaspersky Anti-Virus dessen Verarbeitung, fragt bei Abschluss der Antivirenuntersuchung den Benutzer nach der erforderlichen Aktion und bearbeitet das Objekt.
- Beim Fund eines potentiell gefährlichen Programms erlaubt oder blockiert die Kaspersky Anti-Virus dessen Ausführung und protokolliert entsprechende Informationen.

UPDATE DER ANTIVIREN-DATENBANKEN UND DER PROGRAMMMODULE

Für die Update-Aufgaben der Antiviren-Datenbanken und der Programmmodule sind im Programm standardmäßig folgende Einstellungen vorgesehen:

- Das Update der Antiviren-Datenbanken wird nach Zeitplan alle drei Stunden nach der Installation von Kaspersky Anti-Virus ausgeführt.

Wenn der Computer weniger an einem Tag weniger als drei Stunden arbeitet, werden die Datenbanken sofort aktualisiert, wenn Kaspersky Anti-Virus zum nächsten Mal gestartet wird.

- Das Update der Antiviren-Datenbanken und der Download von eiligen Updates von Kaspersky Anti-Virus werden zugelassen. Vor der Installation der Updates erscheint auf dem Bildschirm eine entsprechende Eingabeaufforderung.

ISOLIERUNG VON VERDÄCHTIGEN OBJEKTEN

Für die Quarantäne sind standardmäßig folgende Einstellungen vorgesehen:

- Die Größe Quarantäne ist nicht beschränkt.
- Die Aufbewahrungsfrist für Objekte in der Quarantäne beträgt 90 Tage.

SICHERHEITSKOPIE VON EINEM INFIZIERTEN OBJEKT

Vor dem Reparieren oder Löschen wird vom Objekt im Backup eine Sicherheitskopie angelegt. Als Standard werden die folgenden Einstellungen verwendet:

- Das Backup ist nicht beschränkt.
- Die Aufbewahrungsfrist für Objekte im Backup beträgt 90 Tage.

4.2. Stufe der Antivirensicherheit

Aus Komfortgründen gibt es eingestellte Optionen für die Antivirensicherheit in der Anwendung in drei Stufen mit Voreinstellungen (s. Tabelle 1):

- **Maximale Sicherheit** – Niveau für den Schutz des Computers, mit dem ein maximal möglicher Schutz bei leicht beeinträchtigter Systemleistung gewährleistet wird.
- **Empfohlen** – Dieses Niveau der Antivirensicherheit basiert auf Empfehlungen der Kaspersky-Lab-Experten und garantiert einen optimalen Schutz Ihres Computers.
- **Maximales Tempo** – Niveau für den Schutz des Computers, auf dem die maximale Arbeitsgeschwindigkeit bei eingeschränkter Menge der zu untersuchenden Objekte gewährleistet wird.

Sollten die Optionen für eine Stufe über die Benutzeroberfläche oder über die Administrationskonsole von Kaspersky Administration Kit 5.0 geändert werden, wechselt der Wert in **Benutzerdefinierte Einstellungen**. Das ist die vierte Stufe der Antivirensicherheit mit individuellen Einstellungen des Benutzers.

Wenn die Parameter über die Administrationskonsole geändert werden, dann wird auf der rechten Seite der Registerkarte **Sicherheit** angezeigt, dass die Einstellungen vom Administrator festgelegt wurden.

In der unten stehenden Tabelle werden die Werte der voreingestellten Sicherheitsstufen für Aufgaben des Echtzeitschutzes (**Sicherheit**) und für den Scan auf Befehl (**Untersuchung**) dargestellt.

Grundkonventionen:

+ Einstellung aktiviert

– Einstellung deaktiviert

x Für diese Aufgabe ist keine Einstellung vorgesehen.

Tabelle 1. Optionen für die Sicherheitseinstellungen

Bezeichnung der Option	Maximale Sicherheit		Empfohlen		Maximales Tempo	
	Schutz	Unter-suchung	Schutz	Unter-suchung	Schutz	Unter-suchung
iChecker verwenden	+	+	+	+	+	+
iStreams verwenden	+	+	+	+	+	+
Untersuchungs-niveau	Dateien nach Format	alle Dateien	Dateien nach Format	alle Dateien	Dateien nach Erweiterung	Dateien nach Format
Größe des zu untersuchenden Objektes unter (MB)	x	–	x	–	x	8
Länge der Untersuchungs-zeit unter (Sek.)	60	–	60	–	60	60
Festplatten	+	x	+	x	+	x
Wechseldaten-träger	+	x	+	x	+	x
Netzdatenträger	+	x	+	x	–	x
NTFS-Streams	+	+	+	+	+	+
Bootsektoren von Datenträgern	+	+	+	+	+	+
Gepackte Dateien	+	+	+	+	+	+
Archive	x	+	x	+	x	–
Selbstent-packende Archive[4]	+	+	–	+	–	+
Mail-Datenbanken	x	+	x	–	x	–
Maildateien in Textformaten	x	+	x	–	x	–
OLE-Objekte	+	+	+	+	–	+

[4] Selbstextrahierende Archive werden nur in ihrem ausführbaren Teil untersucht.

KAPITEL 5. BEDIENUNG DER ANWENDUNG ÜBER LOKALE SCHNITTSTELLE

In diesem Kapitel werden die Arbeit und Einstellungen der Grundaufgaben von Kaspersky Anti-Virus sowie die zusätzlichen Möglichkeiten der Programmbedienung behandelt

5.1. Update der Antiviren-Datenbanken und der Programmmodule

Kaspersky Anti-Virus hat eine Funktion zum automatischen Update der Antiviren-Datenbanken, die Beschreibungen von Viren und deren Behandlungsmethoden enthalten sowie zum Update der Programmmodule von den Update-Servern der Kaspersky Lab.

Die **Aktualisierung der Datenbanken** ist für die Antivirensicherheit Ihres Computers notwendig. Täglich tauchen Hunderte neuer Computerviren auf und jeden Tag nehmen die Experten von Kaspersky Lab Informationen darüber in die Antiviren-Datenbanken auf. Es wird empfohlen, das Update der Antiviren-Datenbanken mindestens alle 3 Stunden vorzunehmen. Bei Virus-Epidemien sollte das Update möglichst häufig, jedoch mindestens einmal stündlich erfolgen.

Zum Download von Updates verwendet Kaspersky Anti-Virus einen der Updateserver von Kaspersky Lab , einen benutzerdefinierten http- oder ftp-Server, oder einen lokalen Ordner oder Netzwerkordner Ihres Computers. Wenn die Verwaltung mit Hilfe von Kaspersky Administration Kit erfolgt, kann das Update aus einem Updateordner erfolgen, der sich auf dem *Administrationsserver* befindet.

Der Download von Updates findet entweder automatisch nach Zeitplan oder manuell statt. Damit die neue Version der Antiviren-Datenbanken rechtzeitig empfangen wird, empfehlen wir, den Zeitplan für einen automatischen Download von Updates einzurichten (Details über die Konfiguration des Zeitplans s. Pkt. 5.8 auf S. 106).

5.1.1. Wann sollen Updates heruntergeladen werden?

Das Programm weist Sie darauf hin, wenn die Antiviren-Datenbanken aktualisiert werden müssen. Sie können sich über den Bedarf für ein Update auch selbst ein Bild machen, indem Sie dessen Status im rechten Teil der Registerkarte Sicherheit (s. Abbildung 2) aufrufen.

Der Updatestatus wird durch folgende Symbole markiert:

Die Antiviren-Datenbanken wurden vor Kurzem oder werden im Moment aktualisiert.

Die Antiviren-Datenbanken benötigen eine Aktualisierung. Wenn das Update aufgrund eines abgelaufenen Lizenzschlüssels nicht möglich ist, bietet Ihnen das Programm Informationen über die Lizenzverlängerung an.

Die Aktualisierung ist dringend erforderlich, weil die Antiviren-Datenbanken stark veraltet, beschädigt oder nicht vorhanden sind.

5.1.2. Manuelles Update. Download von Updates

Um das Update manuell aufzurufen,

klicken Sie auf den Hyperlink Updatedownload im linken Teil der Registerkarte **Sicherheit**;

oder:

auf den Hyperlink Update der Antiviren-Datenbanken *im rechten Teil der Registerkarte* **Sicherheit**, unter Nachrichten über den Status der Antiviren-Datenbanken;

oder:

klicken Sie auf den Punkt **Datenbanken aktualisieren** im Kontextmenü, das sich mit einem Rechtsklick der Maus auf das Programmsymbol in der Taskleiste öffnet.

Durch Klick auf den Hyperlink öffnet sich ein Fenster (s. Abbildung 6) mit Angaben zur Ausführung des Update-Prozesses für die Antiviren-Datenbanken und der Programmmodule.

Der Download-Vorgang für die Updates umfasst folgende Phasen:

1. Kaspersky Anti-Virus überprüft die Netzwerkverbindung und stellt eine Verbindung mit der Updatequelle her.
2. Das Programm empfängt eine Liste sowie die Größe der Updates vom Update-Server bei Kaspersky Lab.
3. Das Programm vergleicht den Status der Antiviren-Datenbanken und Programmmodule auf Ihrem Computer mit dem auf der Updatequelle angebotenen. Sollte auf Ihrem Computer die neueste Version der Antiviren-Datenbanken installiert sein, wird der Updatevorgang beendet. Andernfalls beginnt das Kopieren von Dateien auf Ihren Computer.

   Der Downloadvorgang wird durch einen Kopierindikator dargestellt. Im Feld **Heruntergeladene Updates** wird die Größe der bereits heruntergeladenen Updates angezeigt.

Für die korrekte Installation der heruntergeladenen Updates kann der Neustart des Computers erforderlich sein. In diesem Fall erscheint ein entsprechender Hinweis auf dem Bildschirm.

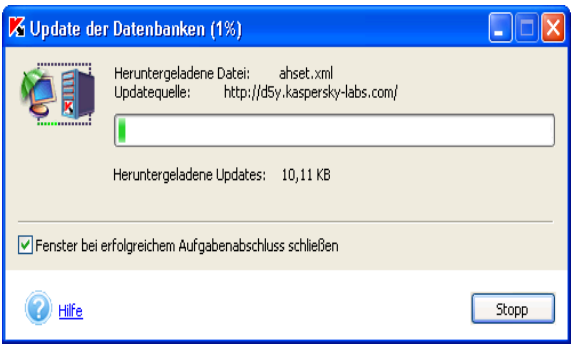

Abbildung 6. Update der Antiviren-Datenbanken und der Anwendungskomponenten

5.1.3. Update-Einstellungen

Um einen Zeitplan für die automatische Aktualisierung der Antiviren-Datenbanken zu erstellen,

klicken Sie auf den Hyperlink Update auf der linken Seite der Registerkarte **Einstellungen** (s. Abbildung 3).

Dadurch wird das Fenster **Update der Antiviren-Datenbanken** geöffnet (s. Abb. 10).

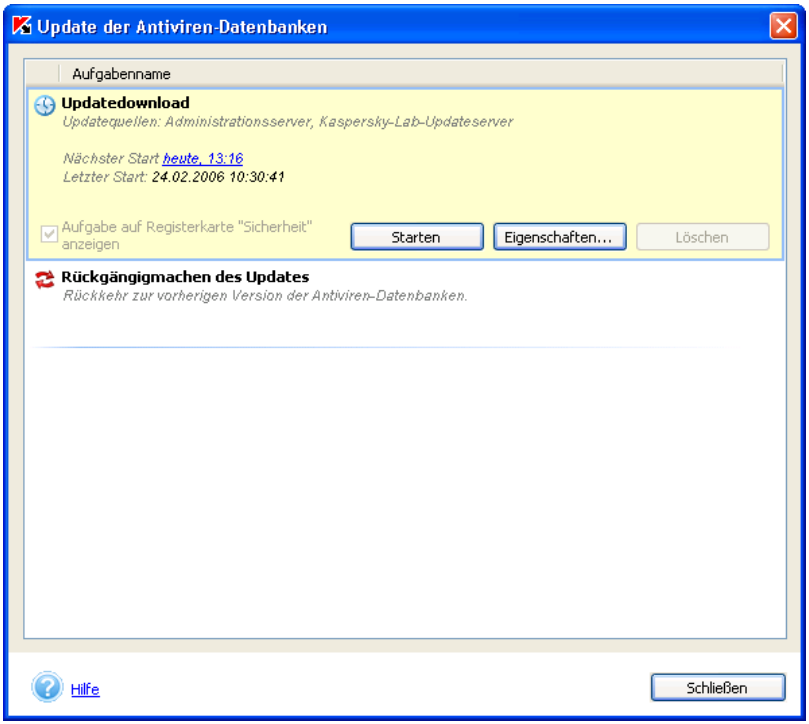

Abbildung 7. Liste der Aufgaben zum Update der Antiviren-Datenbanken

Durch Klick auf den Namen einer Aufgabe wird ein Block geöffnet, der Informationen über die Updatequelle sowie den Zeitpunkt des letzten und nächsten Updatestarts enthält. In diesem Block können Sie mit Hilfe der Schaltfläche **Starten** das Update der Antiviren-Datenbanken manuell starten. Mit Hilfe der Schaltfläche **Éigenschaften** wird das Fenster mit den Update-

Einstellungen für die Antiviren-Datenbanken (s. Abbildung 8) geöffnet, in dem sich folgende Funktionen anpassen lassen:

- den Zeitplan für den automatischen Updatestart konfigurieren (s. Pkt. 5.8 auf S. 106).
- das Update der Programmmodule von Kaspersky Anti-Virus aktivieren (s. Pkt. 5.1.3.1 auf S. 48).
- das Kopieren von Updates in einen lokalen Ordner konfigurieren, aus dem die Updates auf andere Netzwerkcomputer verteilt werden können, auf welchen Kaspersky Anti-Virus installiert ist (s. Pkt. 5.1.3.2 auf S. 50).
- die Updatequelle wählen: Kaspersky-Lab-Server, einen benutzerdefinierten http- oder ftp-Server, einen lokalen Ordner oder einen Netzwerkordner des Computers (s. Pkt. 5.1.3.3 auf S. 51).
- die Proxyserver-Einstellungen festlegen (s. Pkt. 5.1.3.4 auf S. 53).
- den Start der Aufgabe mit den Rechten eines anderen Benutzers konfigurieren (nur für Computer mit dem Betriebssystem Microsoft Windows NT/2K/XP) (s. Pkt. 5.9 auf S. 110).
- den Typ der herunterzuladenden Antiviren-Datenbanken auswählen (s. Pkt. 5.1.3.5 auf S. 55).

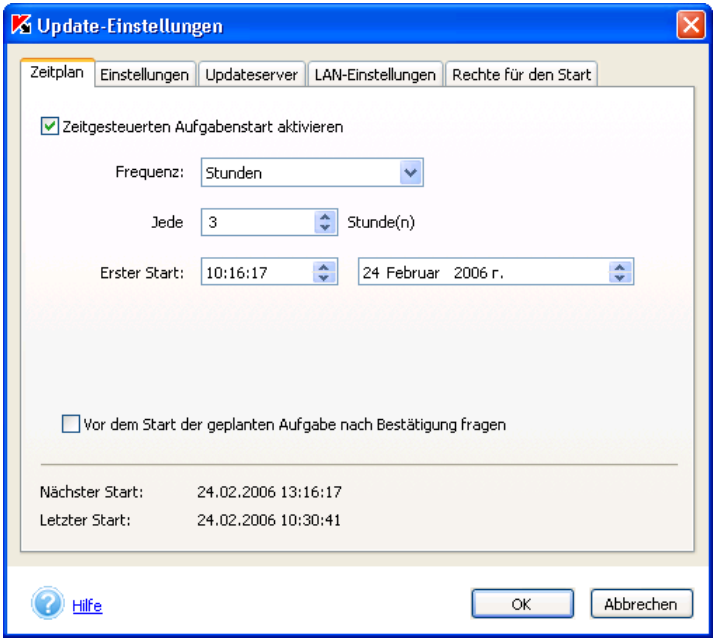

Abbildung 8. Einstellungen für die Aufgabe zum Update der Antiviren-Datenbanken

Die Aufgabe **Rückgängigmachen des Updates** enthält keinerlei Einstellungen. Sie kann nur gestartet werden, um zur vorherigen Version der Antiviren-Datenbanken zurückzukehren.

5.1.3.1. Update der Programmmodule

Neben den Antiviren-Datenbanken können auch die Programmmodule von Kaspersky Anti-Virus aktualisiert werden. Das Update der Programmmodule wird bei Erscheinen auf den Updateservern zur Verfügung gestellt.

Sie können die Programmmodule aus der festgelegten Updatequelle aktualisieren (s. Pkt. 5.1.3.3 auf S. 5.1.3.3). Öffnen Sie dazu auf der Registerkarte **Einstellungen** des Dialogfensters **Update-Einstellungen** (s. Abbildung 9) das Kontrollkästchen **Update der Anwendungsmodule installieren**. Wählen Sie, welche Updates installiert werden sollen:

- **Nur dringende Updates**
- **Alle verfügbaren Updates**

Wenn Sie möchten, dass die Updates der Module nach dem Download automatisch installiert werden, deaktivieren Sie das Kontrollkästchen **Vor der Installation nach Bestätigung fragen**.

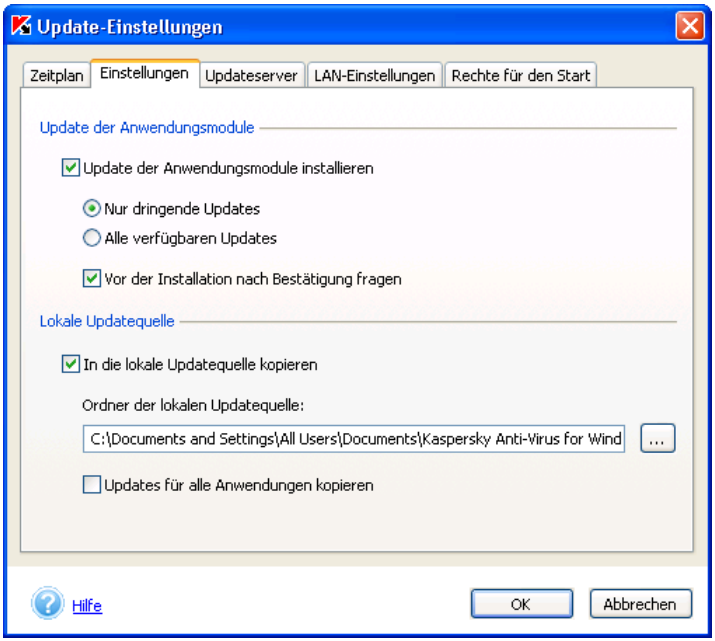

Abbildung 9. Fenster mit Update-Einstellungen.
Registerkarte **Einstellungen**

Wenn Sie bei Kaspersky Lab oder seinen Partnern ein zip-Archiv mit einem Update bestellen, geben Sie unbedingt an, dass Sie auch das Update der Programmmodule erhalten möchten.

Beim Empfang eines Updates für die Anwendungsmodule wird auf dem Bildschirm eine entsprechende Anfrage (s. Abbildung 10) angezeigt. Wählen sie eine der folgenden Varianten:

- **Update für Anwendungsmodule installieren**.
- **Update für Anwendungsmodule nicht installieren und später erinnern** – Beim nächsten Start von Kaspersky Anti-Virus wird an die Installation des Updates für die Programmmodule erinnert.
- **Installation von Updates für Anwendungsmodule deaktivieren** – Bei Auswahl dieser Variante wird das Kontrollkästchen **Update der Anwendungsmodule installieren** auf der Registerkarte **Einstellungen**

des Dialogfensters **Update-Einstellungen** (s. Abbildung 9) deaktiviert und die Aktualisierung der Programmmodule wird abgeschaltet.

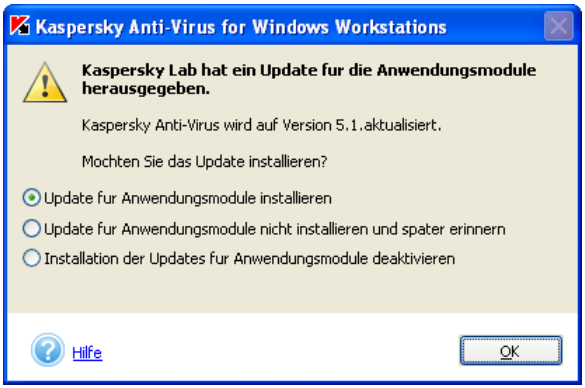
Kaspersky Anti-Virus for Windows Workstations
Kaspersky Lab hat ein Update fur die Anwendungsmodule herausgegeben.
Kaspersky Anti-Virus wird auf Version 5.1.aktualisiert.
Mochten Sie das Update installieren?
Update fur Anwendungsmodule installieren
Update fur Anwendungsmodule nicht installieren und spater erinnern
Installation der Updates fur Anwendungsmodule deaktivieren
Hilfe
OK

Abbildung 10. Anfrage zur Installation von Updates für die Anwendungsmodule

5.1.3.2. Kopieren von Updates in einen lokalen Ordner

Auf der Registerkarte **Einstellungen** (s. Abbildung 9) können Sie die Arbeit des Kopierdiensts für Updates anpassen. Mit diesem Dienst können die von den Kaspersky-Lab-Servern heruntergeladenen Updates der Antiviren-Datenbanken und Programmmodule für die Anwendung in einem lokalen Ordner abgelegt werden, um danach auf andere Netzwerkcomputer verteilt zu werden (auf denen Kaspersky Anti-Virus installiert ist). Dadurch lassen sich Internetressourcen einsparen.

Um den Kopierdienst für Updates anzuschalten, aktivieren Sie das Kontrollkästchen **In die lokale Updatequelle kopieren**. Geben Sie im Feld **Ordner der lokalen Updatequelle** den Pfad des Ordners an.

Daneben können Sie auch die Methode zum Kopieren der Updates wählen:

- *vollständig* – In diesem Fall werden die Antiviren-Datenbanken und die Updates für Module für alle Kaspersky-Lab-Anwendungen kopiert. Um das vollständige Update zu wählen, aktivieren Sie das Kontrollkästchen **Updates für alle Anwendungen kopieren**.
- *benutzerdefiniert* – Bei dieser Variante werden nur die Antiviren-Datenbanken und die Updates für Module von Kaspersky Anti-Virus 5.0 for Windows Workstations und für Kaspersky Anti-Virus 5.0 for Windows File Servers kopiert. Um diese Updatemethode zu wählen, deaktivieren

Sie das Kontrollkästchen **Updates für alle Anwendungen kopieren** (diese Einstellung gilt als Standard).

5.1.3.3. Auswahl der Updatequelle

Die Auswahl der Update-Quelle erfolgt auf der Registerkarte **Updateserver** des Dialogfensters **Update-Einstellungen** (s. Abbildung 11).

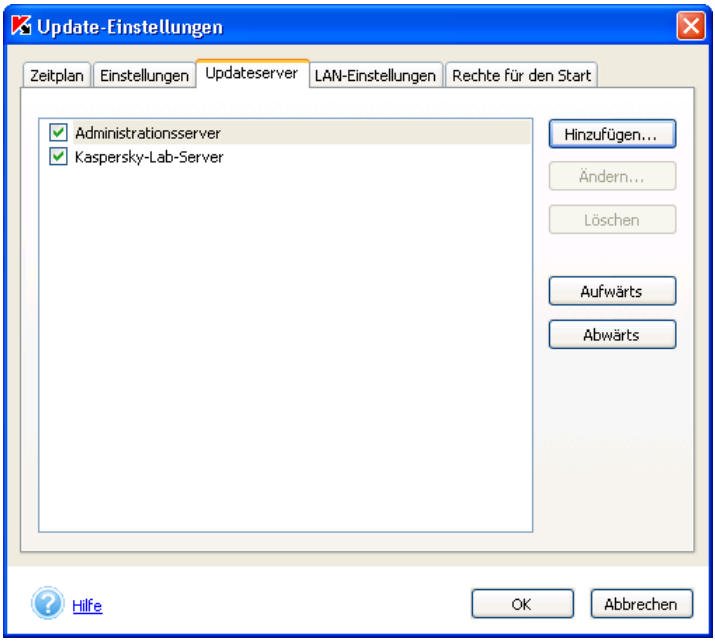

Abbildung 11. Fenster für Update-Einstellungen.
Registerkarte **Updateserver**

Als Ressource, aus welcher das Update erfolgt, kann festgelegt werden:

- *Administrationsserver* – zentraler Updatespeicher, der sich auf dem Administrationsserver für Kaspersky Administration Kit befindet. Diese Updatequelle steht nicht zur Verfügung, wenn der Administrationsagent nicht auf dem Computer installiert ist (Details s. Hilfesystem für Kaspersky Administration Kit 5.0).
- *Kaspersky-Lab-Server* – Internetseiten von Kaspersky Lab, auf denen die aktualisierten Antiviren-Datenbanken und Programmmodule zur Verfügung gestellt werden.

- ftp- oder http-Server, die vom Benutzer hinzugefügt werden und die aktuellen Updates enthalten.
- ein lokaler Ordner oder ein Netzwerkordner.

Standardmäßig erfolgt das Update von den Kaspersky-Lab-Updateservern über das Internet bzw. bei der Arbeit mit Kaspersky Administration Kit 5.0 vom Administrationsserver. Sie können die Liste erweitern und zusätzliche Updatequellen hinzufügen. Klicken Sie dazu auf die Schaltfläche **Hinzufügen** und wählen Sie den Typ der Quelle aus: *Adresse des Updateservers* oder *Ordner*. Bei Auswahl der Variante *Adresse des Updateservers* geben Sie im folgenden Fenster die Adresse des ftp- oder http-Servers an (Der Servername muss mit dem Protokollpräfix angegeben werden, das Sie verwenden möchten, beispielsweise: *http://server.net* oder *ftp://10.0.0.1*). Geben Sie bei der Auswahl der Variante *Ordner* den Pfad des Ordners an, der die Updates enthält.

Mit Hilfe der Schaltfläche **Ändern** können Sie die Einstellungen für die Updatequelle anpassen. Für den Quellentyp *Adresse des Updateservers* können Sie die Adresse ändern, für den Quellentyp *Ordner* den Pfad.

Sie können den Standort des Kaspersky-Lab-Servers festlegen, von dem die Updates kopiert werden sollen. Wählen Sie dazu aus der Dropdown-Liste **Ort** (s. Abbildung 12) das entsprechende Land aus. In der Grundeinstellung wird das Land auf Basis der Regionsoptionen des Betriebssystems ermittelt. Geben Sie zur Ermittlung des geografisch nächstliegenden Updateservers Ihren gegenwärtigen Aufenthaltsort an. Dadurch lässt sich die Dauer des Updates verkürzen und die Downloadgeschwindigkeit erhöhen. Außerdem können Sie die Verwendung eines Proxyservers abschalten, indem Sie das entsprechende Kontrollkästchen deaktivieren.

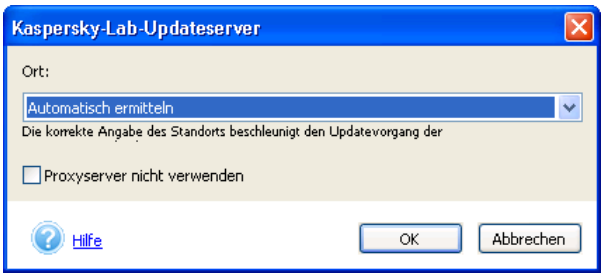

Abbildung 12. Ändern der Parameter für die Updatequelle. Auswahl des Serverstandorts

Damit das Update aus der angegebenen Quelle erfolgt, aktivieren Sie das entsprechende Kontrollkästchen. Es können gleichzeitig mehrere Ressourcen gewählt werden. In diesem Fall führt Kaspersky Anti-Virus die Aktualisierung aus der ersten Quelle der Liste aus. Wenn aus irgendeinem Grund kein Zugriff auf diese Quelle besteht, erfolgt das Update aus der folgenden Quelle der Liste,

usw. Mit Hilfe der Schaltflächen **Aufwärts**/**Abwärts** können Sie die Reihenfolge der Updatequellen in der Liste ändern.

Wenn Sie keinen Zugriff auf die Kaspersky-Lab-Updateserver besitzen (wenn beispielsweise kein Internetzugang vorhanden ist), können Sie unsere Zentralverwaltung unter der Nummer +7 (495) 797-87-00 anrufen. Dort können Sie die Adressen der Partner von Kaspersky Lab erfahren, die Ihnen die Antiviren-Datenbanken auf Disketten oder CDs im zip-Format zur Verfügung stellen können.

Bitte denken Sie daran, bei der Bestellung von Antiviren-Datenbanken anzugeben, welchen Typ der Datenbanken Sie erhalten möchten: Standard- oder erweiterte Datenbanken (s. Pkt. 5.1.3.5 auf S. 55).

Entpacken Sie das zip-Archiv mit den gelieferten Antiviren-Datenbanken in einem Ordner Ihres Computers und legen Sie diesen Ordner als Updatequelle fest.

5.1.3.4. Konfiguration des Proxyservers

Die Konfiguration der Netzwerkverbindung erfolgt auf der Registerkarte **LAN-Einstellungen** (s. Abbildung 13). Zum Ermitteln der Proxyserver-Einstellungen stehen zwei Methoden zur Auswahl:

- **Proxyserver-Einstellungen automatisch erkennen**
- **Folgenden Proxyserver verwenden**

Die erste Variante ist standardmäßig gewählt und die Proxyserver-Einstellungen werden aus Microsoft Internet Explorer übernommen. Wenn der Proxyserver eine Autorisierung erfordert, wählen Sie die zweite Variante und geben Sie die Parameter des Proxyservers manuell an:

Adresse – IP-Adresse des Proxyservers im Dezimalformat (z.B. *10.10.10.102*) oder Name des Proxyservers.

Port – Nummer des Ports, den der Proxyserver verwendet. Wählen Sie einen Wert aus der Dropdown-Liste aus (*3128*, *8080*, *8082*, *8903)* oder geben Sie den Wert manuell an.

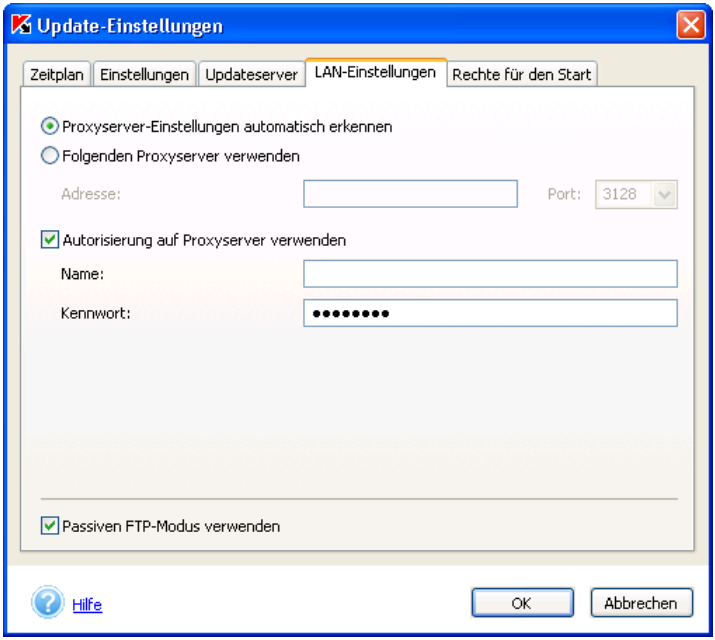

Abbildung 13. Proxyserver-Einstellungen

Wenn der Proxyserver eine Autorisierung fordert, aktivieren Sie das Kontrollkästchen **Autorisierung auf Proxyserver verwenden** und geben Sie in den unten angebrachten Feldern den erforderlichen Benutzernamen und das Kennwort an.

Wenn der Proxyserver die Autorisierung erfordert, Sie aber Namen und Kennwort nicht angegeben haben oder die angegebenen Daten aus irgendeinem Grund vom Proxyserver nicht akzeptiert wurden, erfolgt beim Start des Updates eine Eingabeaufforderung nach Namen und Kennwort für die Autorisierung. Wenn die Autorisierung erfolgreich verläuft, werden der angegebene Name und das Kennwort beim nächsten Update verwendet. Andernfalls werden die Autorisierungsparameter erneut erfragt.

Wenn auf Ihrem Server eine Firewall installiert ist und die Verbindung mit einer FTP-Seite im aktiven Modus nicht möglich ist, aktivieren Sie das Kontrollkästchen **Passiven FTP-Modus verwenden**.

5.1.3.5. Auswahl des Typs der Antiviren-Datenbanken

Kaspersky Anti-Virus bietet Ihnen die Wahl zwischen zwei Typen von Antiviren-Datenbanken, die vom Programm bei der Arbeit verwendet werden:

- Die *Standard-Datenbanken* enthalten Einträge über alle im Moment bekannten böswilligen Programme und die entsprechenden Desinfektionsmethoden.
- Wenn Sie die Daten auf Ihrem Computer vor potentiell gefährlichen Programmen schützen möchten, verwenden Sie die *Erweiterten Datenbanken*. Diese enthalten Erweitertzu den Einträgen der Standard-Datenbanken auch die Beschreibung von Adware, Spyware, Hacker-Dienstprogrammen und anderer potentiell gefährlicher Software.

Um den normalen Antivirenschutz Ihres Computers zu gewährleisten, sind die Standard-Antiviren-Datenbanken völlig ausreichend. Die Verwendung der erweiterten Datenbanken kann sich auf die Funktionsgeschwindigkeit von Kaspersky Anti-Virus auswirken. Außerdem können bestimmte von Ihnen verwendete Softwareprodukte als potentiell gefährliche Programme eingestuft werden.

Um den Typ der Datenbanken auszuwählen, die Kaspersky Anti-Virus bei der Arbeit verwenden sollen,

1. Benutzen Sie den Hyperlink Bedrohungen und Ausnahmen auf der linken Seite der Registerkarte **Einstellungen** (s. Abbildung 3).
2. Aktivieren Sie im folgenden Dialogfenster (s. Abbildung 14) im Abschnitt **Erkennbare Bedrohungen** das Kontrollkästchen **Adware, Riskware, Dialer und andere gefährliche Software**, wenn Sie die erweiterten Antiviren-Datenbanken verwenden möchten. Um zum vermeiden, dass Programme, die Sie verwenden, gelöscht werden, wird empfohlen, eine Aktion für gefährliche Objekte festzulegen, der eine Bestätigung des Benutzers vorausgeht (s. Pkt. 5.2.2.2 auf S. 68).

Das Kontrollkästchen **Viren, Würmer, Trojaner und Hackerprogramme, Spyware** ist standardmäßig aktiviert und kann nicht deaktiviert werden. Es zeigt an, dass bei der Untersuchung die Standard-Antiviren-Datenbanken verwendet werden.

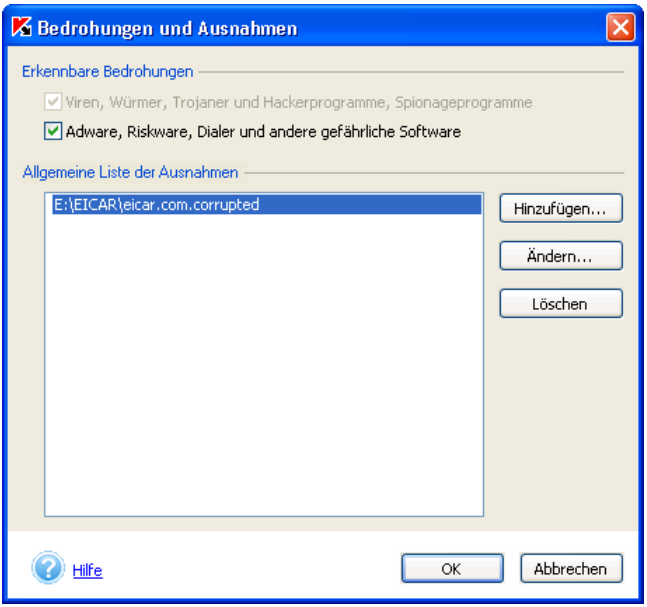

Abbildung 14. Auswahl des Typs der Antiviren-Datenbanken

5.2. Echtzeitschutz

Der Echtzeitschutz Ihres Computers wird nur dann gewährleistet, wenn Sie bei der Programminstallation seine Verwendung nicht abgelehnt haben.

Echtzeitschutz – In diesem Modus kontrolliert Kaspersky Anti-Virus ständig alle Zugriffe auf Objekte der Dateisysteme, ein- und ausgehende E-Mails sowie Aktionen der potentiell gefährlichen Skripte VBScript, JavaScript und Makrobefehle, die von Office-Anwendungen genutzt werden, und erkennt potentiell gefährliche Programme.

Wenn ein Objekt von einem Benutzer oder Programm zum Lesen/Schreiben geöffnet wird, untersucht die Anwendung es auf Virenbefall. Wenn ein Virus gefunden wird, führt die Anwendung die Desinfektion des infizierten Objekts aus oder blockiert den Zugriff auf das Objekt (je nach den von Ihnen vorgenommenen Einstellungen). Dadurch kann die Anwendung schädlichen Code erkennen und neutralisieren, bevor es zu einer wirklichen Infektion des Systems kommt.

Im Echtzeitschutzmodus erfüllt das Programm mehrere Funktionen:

- Echtzeitschutz für Dateien (s. Pkt. 5.2.1 auf S. 59)
- Echtzeitschutz für elektronische Post (s. Pkt. 5.2.2 auf S. 64)
- Untersuchung von VBA-Makros (s. Pkt. 5.2.4 auf S. 70)
- Echtzeituntersuchung von Skripts (s. Pkt. 5.2.5 auf S. 72)
- Echtzeitschutz vor Netzwerk-Angriffen (s. Pkt. 5.2.6 auf S. 74)

Jede dieser Funktionen kann separat konfiguriert oder deaktiviert werden, was keinen Einfluss auf die Arbeit der anderen Echtzeitschutzkomponenten ausübt.

Informationen über den aktuellen Zustand des Echtzeitschutzes befinden sich auf der rechten Seite der Registerkarte **Sicherheit** (s. Abbildung 2) des Programmhauptfensters.

Der Zustand des Echtzeitschutzes wird durch folgende Symbole dargestellt:

Der Echtzeitschutz ist aktiviert, die Einstellungen entsprechen der empfohlenen Sicherheitsstufe.

Der Echtzeitschutz ist aktiviert, aber die Einstellungen weichen von der empfohlenen Sicherheitsstufe ab.

Der Antivirenschutz wurde angehalten. Dieser Zustand bedeutet, dass der Schutz Ihres Computers vorübergehend deaktiviert wurde.

Der Echtzeitschutz funktioniert nicht. In diesem Fall wird empfohlen, die Parameter des Echtzeitschutzes anzupassen und ihn neu zu starten.

Der Echtzeitschutz ist ab dem Start des Betriebssystems und bis zum Ausschalten des Computers aktiv. Während der Arbeit können Situationen eintreten, in denen der Echtzeitschutz angehalten werden muss. Öffnen Sie dazu das Kontextmenü von Kaspersky Anti-Virus und wählen Sie den Punkt **Echtzeitschutz anhalten** (s. Abbildung 1).

Da vor dem vollständigen Ausschalten des Antivirenschutzes gewarnt wird, bietet Kaspersky Anti-Virus Ihnen an, ihn vorübergehend zu deaktivieren.

Um den Echtzeitschutzmodus anzuhalten,

wählen Sie im Fenster **Echtzeitschutz anhalten** (s. Abbildung 15) eine der folgenden Varianten:

- **In 5/10/15 Minuten –** Der Schutz wird nach Ablauf des festgelegten Zeitraums wieder aktiviert.
- **Bei der nächsten Netzwerkverbindung** – Der Schutz wird sofort aktiviert, wenn der Computer eine Netzwerkverbindung aufbaut (Diese Variante erscheint in der Liste, wenn in diesem Moment keine Netzwerkverbindung besteht).
- **Beim nächsten Start von Kaspersky Anti-Virus** – Der Schutz wird aktiviert, wenn das Programm aus dem Menü **Start → Programme → Kaspersky Anti-Virus for Windows Workstations** gestartet wird oder nach dem Neustart des Systems (unter der Voraussetzung, dass der Modus zum Programmstart bei Systemstart aktiviert ist).
- **Nur auf Befehl des Benutzers** – Der Schutz wird erst dann aktiviert, wenn Sie ihn selbst starten. Um den Schutz zu starten, wählen Sie im Kontextmenü von Kaspersky Anti-Virus den Punkt **Echtzeitschutz aktivieren**.

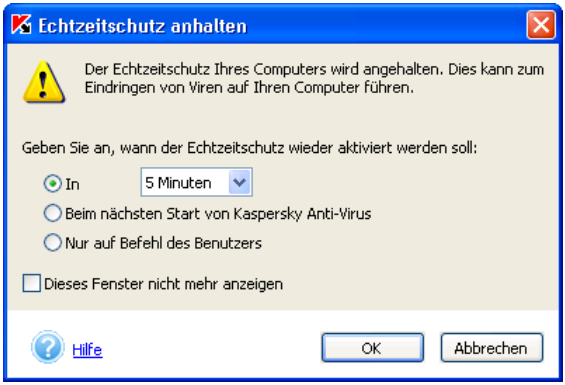
Echtzeitschutz anhalten
Der Echtzeitschutz Ihres Computers wird angehalten. Dies kann zum Eindringen von Viren auf Ihren Computer führen.
Geben Sie an, wann der Echtzeitschutz wieder aktiviert werden soll:
In
5 Minuten
Beim nächsten Start von Kaspersky Anti-Virus
Nur auf Befehl des Benutzers
Dieses Fenster nicht mehr anzeigen
Hilfe
OK
Abbrechen

Abbildung 15. Vorübergehendes Ausschalten des Antivirenschutzes

Durch d Deaktivieren des Echtzeitschutzmodus wird das Risiko einer Vireninfektion Ihres Computers wesentlich erhöht. Trotzdem können Sie den Echtzeitschutz beim Ausführen bestimmter Operationen (beispielsweise beim Defragmentieren eines Laufwerks mit FAT32-Dateisystem) ausschalten, um Zeit zu sparen.

Bei Bedarf können Sie nicht den gesamten Schutz beenden, sondern nur einzelne Anwendungskomponenten: Schutz des Dateisystems (s. Pkt. 5.2.1 auf S. 59), E-Mail-Schutz (s. Pkt. 5.2.2 auf S. 64), Makro-Untersuchung (s. Pkt. 5.2.4 auf S. 70), Skriptuntersuchung (s. Pkt. 5.2.5 auf S. 72) oder Schutz vor Netzwerk-Angriffen (s. Pkt. 5.2.6 auf S. 74).

Um die Einstellungen für den Echtzeitschutzmodus zu überprüfen oder zu ändern:

verwenden Sie den Hyperlink Echtzeitschutz auf er linken Seite der Registerkarte **Einstellungen** (s. Abbildung 3).

Das Fenster mit den Einstellungen des Echtzeitschutzes ist entsprechend den Schutzfunktionen unterteilt. Im Folgenden wird die Konfiguration jeder Funktion ausführlich beschrieben.

5.2.1. Untersuchung des Dateisystems

Wenn der Datei-Schutz installiert und aktiviert ist, analysiert Kaspersky Anti-Virus im Echtzeitschutz-Modus den Zugriff auf das Dateisystem des Computers hinsichtlich des Vorhandenseins von schädlichem Code.

Die Einstellung des Echtzeitschutzes für das Dateisystem wird im Fenster **Echtzeitschutz-Einstellungen** auf der Registerkarte **Dateien** (s. Abbildung 16) vorgenommen. In diesem Fenster können Sie:

- den Schutz aktivieren/deaktivieren. Aktivieren oder deaktivieren Sie dazu das Kontrollkästchen **Dateisystem-Echtzeitschutz aktivieren**. Das Kontrollkästchen und der Schutz sind standardmäßig aktiviert.
- die Stufe der Antivirensicherheit festlegen und die gewählte Sicherheitsstufe detailliert anpassen (s. Pkt. 5.2.1.1 auf S. 60).
- eine Liste der Objekte erstellen, die beim Echtzeitschutz für Dateien nicht untersucht werden sollen (s. Pkt. 5.7 auf S. 102). Verwenden Sie den Hyperlink nicht festgelegt/ festgelegt neben dem Parameter **Ausnahmen** in der Beschreibung der geltenden Schutzeinstellungen, um in das Fenster zum Erstellen der Ausnahmenliste zu gelangen. Das Aussehen des Hyperlinks ist davon abhängig, ob Ausnahmen festgelegt sind oder nicht.
- eine Liste der vertrauenswürdigen Prozesse erstellen, deren Dateiaktivität im Echtzeitschutz für Dateien nicht untersucht wird (s. Pkt. 5.5 auf S. 99);
- die Aktion festlegen, die von Kaspersky Anti-Virus beim Fund gefährlicher und verdächtiger Objekte angewandt werden soll (s. Pkt. 5.2.1.2 auf S. 62).

Wenn der Echtzeitschutz für Dateien nicht installiert ist, stehen die oben genannten Parameter nicht zur Verfügung. Um den Datei-Schutz zu installieren, ist die Neuinstallation des Programms erforderlich.

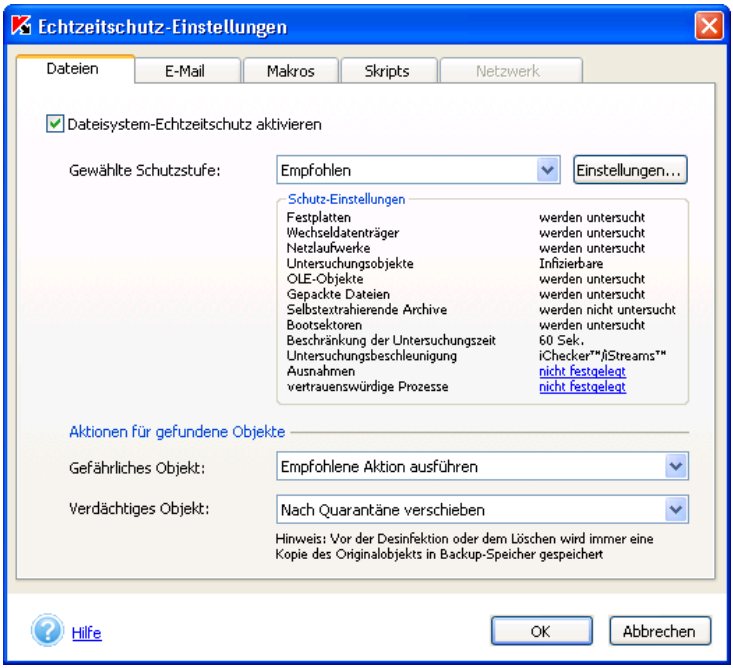

Abbildung 16. Einstellungen der Aufgabe zum Schutz von Objekten des Dateisystems

5.2.1.1. Auswahl der Sicherheitsstufe

Wählen Sie in der Dropdown-Liste **Gewählte Schutzstufe** eine der drei von Kaspersky-Lab-Experten vordefinierten Stufen (Details s. Kapitel 4 auf S. 38). Standardmäßig gelten die Einstellungen der empfohlenen Sicherheitsstufe.

Sie können auf der Basis jeder Sicherheitsstufe eigene Einstellungen vornehmen. Dabei ändert sich die Sicherheitsstufe in **Benutzerdefinierte Einstellungen**. Bei der Rückkehr zu einer der drei vordefinierten Stufen werden die benutzerdefinierten Einstellungen nicht gespeichert.

Die Parameter der gewählten Sicherheitsstufe können im Fenster **Einstellungen für Datei-Echtzeitschutz** (s. Abbildung 17) überprüft und geändert werden. Dieses Fenster wird durch die Schaltfläche **Einstellungen** auf der Registerkarte **Dateien** geöffnet (s. Abbildung 16).

Aktivieren Sie im Abschnitt **Untersuchungsbereich** die Kontrollkästchen, durch welche die zu untersuchenden Laufwerke festgelegt werden.
Wählen Sie im Abschnitt **Untersuchungsobjekte** die Objekte, welche untersucht werden sollen:

- **Alle Objekte untersuchen** – Dateien untersuchen, ohne Berücksichtigung des Typs und der Erweiterung.
- **Nur infizierbare Objekte untersuchen** – Dateien untersuchen, die potentiell infiziert werden können; die Analyse der Infizierbarkeit basiert auf der internen Dateistruktur.
- **Objekte nach Erweiterung untersuchen** – Dateien untersuchen, die potentiell infiziert werden können; die Analyse der Infizierbarkeit basiert auf der Dateinamenserweiterung.

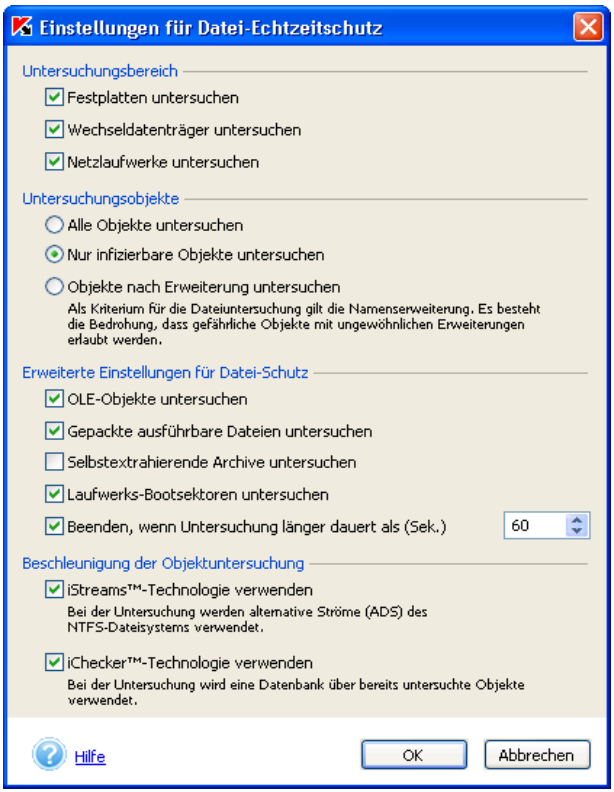

Abbildung 17. Detailliertes Anpassen des Echtzeitschutzes für Dateien

Begrenzen Sie im Abschnitt **Erweiterte Einstellungen für Datei-Schutz** die Untersuchungszeit eines Objekts. Legen Sie dazu für das Untersuchungsintervall einen Wert (in Sekunden) fest und bestimmen Sie, ob folgende Objekte untersucht werden sollen:

- angehängte oder in andere Dateien eingebettete Objekte (OLE-Objekte)
- gepackte ausführbare Dateien
- selbstextrahierende Archive
- Laufwerksbootsektoren

Im Abschnitt **Beschleunigung der Objektuntersuchung** können Sie die Verwendung von Technologien iChecker™ und iStreams™ zur Beschleunigung der Antivirenuntersuchung aktivieren/deaktivieren. Aktivieren Sie die entsprechenden Kontrollkästchen, damit die Technologien verwendet werden.

Wenn Sie die Verwendung der Technologie iStreams™ bei der Programminstallation abgelehnt haben, ist die Neuinstallation von Kaspersky Anti-Virus erforderlich, um iStreams™ zu aktivieren. Erst danach stehen die Einstellungen für diese Technologie zur Verfügung.

5.2.1.2. Auswahl der Aktion für gefundene Objekte

Legen Sie im Abschnitt **Aktionen für gefundene Objekte** (s. Abbildung 16) die Aktion fest, die Kaspersky Anti-Virus beim Fund von gefährlichen und verdächtigen Objekten ausführen soll:

- **Benutzer nach Aktion fragen** – Der Zugriff auf das Objekt wird gesperrt und auf dem Bildschirm wird eine Anfrage über die auszuführende Aktion für das Objekt angezeigt. Dieser Modus gilt als Standard.

  Wenn das Programm innerhalb von 30 Sekunden nach der Eingabeaufforderung keine Antwort von Ihnen erhält, wird die empfohlene Aktion auf das Objekt angewandt. Für jeden gefundenen Objekttyp wird eine bestimmte Aktion empfohlen.

  Es folgt eine Liste aller möglichen Aktionen, die Kaspersky Anti-Virus zur Auswahl anbietet (Die Liste der Aktionen kann für jeden Objekttyp unterschiedlich sein):

  - *Desinfizieren* des infizierten Objekts.
  - *Nach Quarantäne verschieben*: Das möglicherweise von einem Virus oder dessen Modifikation infizierte Objekt in die Quarantäne verschieben.

Es kann vorkommen, dass nach dem Verschieben einer Datei in die Quarantäne auf dem Bildschirm eine Meldung darüber erscheint, dass das Objekt nicht gelöscht werden kann. Der Grund liegt darin, dass Objekte beim Verschieben in die Quarantäne verschoben werden, d.h. sie werden in die Quarantäne kopiert und am ursprünglichen Speicherort gelöscht. Allerdings kann beim Verschieben nicht jedes Objekt gelöscht werden (z.B. ein Objekt, das momentan von einem anderen Programm verwendet wird).

  - *Löschen* des gefährlichen Objekts, wenn seine Desinfektion fehlgeschlagen oder nicht möglich ist.
  - *Überspringen* – Keine Aktionen mit dem Objekt vornehmen. Es werden nur Informationen über den Fund im Protokoll über die Programmarbeit aufgezeichnet.

- **Empfohlene Aktion ausführen** – Der Zugriff auf das Objekt wird gesperrt und die für dieses Objekt empfohlene Aktion ausgeführt. Für infizierte Objekte ist die empfohlene Aktion *Desinfizieren*, *irreparable Objekte löschen*[5], für möglicherweise infizierte Objekte ist es *Verschieben nach Quarantäne* und für Trojanische Programme und Würmer ist es *Löschen*. Wenn ein infiziertes / möglicherweise infiziertes Objekt als potentiell gefährliches Programm gilt, wird der Zugriff auf das Objekt *gesperrt*.
- **Zugriff verbieten, desinfizieren, irreparable Objekte löschen** – Das Objekt wird gesperrt und die Desinfektion wird versucht. Wenn die Desinfektion nicht möglich ist, wird es ohne vorherige Eingabeaufforderung gelöscht. Bei der Desinfektion wird eine Kopie des Objekts im Backup aufbewahrt.
- **Zugriff verbieten und Objekt löschen** – Der Zugriff auf das Objekt wird gesperrt und das Objekt wird ohne zusätzliche Benachrichtigung des Benutzers gelöscht. Beim Löschen wird eine Kopie des Objekts in Backup gespeichert.
- **Nur Zugriff verbieten** – Der Zugriff auf das Objekt wird gesperrt und es wird keine Anfrage nach der Bearbeitung des Objekts auf dem Bildschirm angezeigt. Informationen werden protokolliert.
- **Nach Quarantäne verschieben** (nur für verdächtige Objekte) – Der Zugriff auf das Objekt wird gesperrt und das Objekt wird in die

[5] Standardmäßig werden infizierte Objekte des Arbeitsspeichers gelöscht, wogegen vireninfizierte Bootsektoren der Desinfektion unterzogen und gesperrt werden, falls die Desinfektion nicht möglich ist.

Quarantäne verschoben, um später unter Verwendung von aktualisierten Antiviren-Datenbanken einer zusätzlichen Untersuchung unterzogen, wiederhergestellt, zur Analyse an Kaspersky Lab eingesandt oder gelöscht zu werden.

5.2.2. E-Mail-Untersuchung

Der Echtzeitschutz für eingehende und ausgehende E-Mails wird nur dann gewährleistet, wenn Sie seine Verwendung bei der Programminstallation nicht abgelehnt haben. Um den Mail-Schutz zu installieren, ist die Neuinstallation des Programms erforderlich.

Im Echtzeitschutz analysiert Kaspersky Anti-Virus Anfragen zum Empfang und Versand von elektronischer Post, verhindert den Angriff durch schädlichen Code auf Ihren Posteingang sowie den Versand von verdächtigen oder infizierten Objekte an Ihre Adressaten.

Kaspersky Anti-Virus erledigt folgende Aufgaben:

- Abfangen ein- und ausgehender E-Mail-Nachrichten nach den SMTP- und POP3-Protokollen für beliebige Mailclients;
- Abfangen ein- und ausgehender E-Mail-Nachrichten bei der Verwaltung durch den Mailclient Microsoft Office Outlook mit beliebigen Mailprotokollen;
- Auffinden von verdächtigen und infizierten Objekten im Nachrichtenkörper und in beigefügten Objekten mit beliebiger Verschachtelung.

Bei Untersuchung der E-Mails werden standardmäßig die Einstellungen der empfohlenen Stufe für die Antivirensicherheit mit folgenden Einstellungen verwendet:

- eingehende Post nach POP3-Protokoll untersuchen;
- angehängte Archive und Mailformate untersuchen.

Beachten Sie, dass als Standard mit dem SMTP-Protokoll ausgehende Mails nicht untersucht werden.

Der E-Mail-Echtzeitschutz wird auf der Registerkarte **E-Mail** des Dialogfensters **Echtzeitschutz-Einstellungen** angepasst (s. Abbildung 18). Hier können Sie:

- den Schutz aktivieren/deaktivieren. Aktivieren oder deaktivieren Sie das Kontrollkästchen ☑ **E-Mail-Echtzeitschutz aktivieren**. Das Kontrollkästchen ist standardmäßig aktiviert und der Schutz angeschaltet.

- die Stufe der Antiviren-Sicherheit festlegen und die gewählte Stufe detailliert anpassen (s. Pkt. 5.2.2.1 auf S. 66).
- eine Liste der Objekte anlegen, die beim E-Mail-Echtzeitschutz nicht untersucht werden sollen (s. Pkt. 5.7 auf S. 102). Um in das Fenster zum Erstellen der Ausnahmenliste zu gelangen, klicken Sie in der Beschreibung der geltenden Schutzparameter auf den Hyperlink nicht festgelegt/ festgelegt neben dem Parameter **Ausnahmen**. Das Aussehen des Hyperlinks hängt davon ab, ob Ausnahmen festgelegt wurden oder nicht.
- die Aktion festlegen, die von Kaspersky Anti-Virus beim Fund von gefährlichen und verdächtigen Objekten ausgeführt werden soll (s. Pkt. 5.2.1.2 auf S. 62).

Zur Untersuchung von E-Mails in Microsoft Office Outlook wurde ein spezielles Modul entwickelt, das sich in das Programm einbindet. Bei der Installation von Kaspersky Anti-Virus erscheint in Microsoft Office Outlook im Menü Extras unter Optionen eine zusätzliche Registerkarte (Details s. Punkt 5.2.3 auf S. 69).

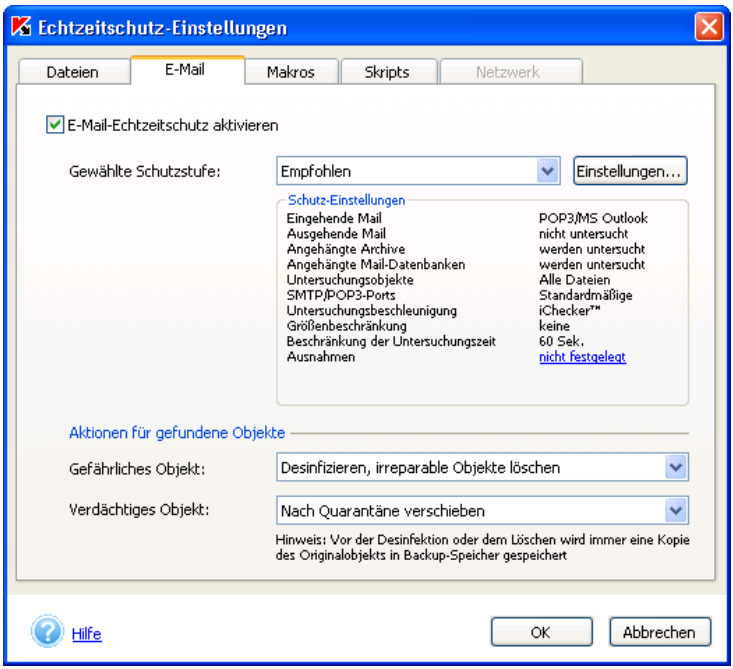

Abbildung 18. Parameter der Aufgabe für den E-Mail-Schutz

5.2.2.1. Auswahl der Sicherheitsstufe

Wählen Sie in der **Dropdown**-Liste **Gewählte Schutzstufe** eine der drei von Kaspersky-Lab-Experten vordefinierten Stufen (Details s. Kapitel 4 auf S. 38). Standardmäßig gelten die Einstellungen der empfohlenen Sicherheitsstufe.

Sie können auf der Basis jeder Sicherheitsstufe eigene Einstellungen vornehmen. Dabei ändert sich die Sicherheitsstufe in **Benutzerdefinierte Einstellungen**. Bei der Rückkehr zu einer der drei vordefinierten Stufen werden die benutzerdefinierten Einstellungen nicht gespeichert.

Die Parameter der gewählten Sicherheitsstufe können im Fenster **Einstellungen für E-Mail-Echtzeitschutz** (s. Abb. 19) überprüft und geändert werden. Dieses Fenster wird durch die Schaltfläche **Einstellungen** auf der Registerkarte **E-Mail** (s. Abbildung 18) geöffnet.

Im oberen Teil der Registerkarte befinden sich Kontrollkästchen, durch welche die Untersuchungsobjekte festlegt werden. Wenn ein Kontrollkästchen aktiviert ist, führt das Programm das Abfangen und die Untersuchung der entsprechenden Objekte aus:

- **Nach POP3-Protokoll empfangene Mail untersuchen** – Untersuchung von eingehender Mail, die nach dem Protokoll POP3 übertragen wird, für jedes beliebige Mailprogramm.
- **Eingehende Microsoft Office Outlook Mail untersuchen** – Untersuchung von eingehender Mail bei der Arbeit mit dem Mailprogramm Microsoft Office Outlook für jedes beliebige Mailprotokoll.
- **Nach SMTP-Protokoll gesendete Mail untersuchen** – Untersuchung von ausgehender Mail, die nach dem Protokoll SMTP übertragen wird, für jedes beliebige Mailprogramm.
- **Ausgehende Microsoft Office Outlook Mail untersuchen** – Untersuchung von ausgehender Mail bei der Arbeit mit dem Mailprogramm Microsoft Office Outlook für jedes beliebige Mailprotokoll.
- **Angehängte Archive untersuchen** – Untersuchung von an eine Nachricht angehängten Archiven.

  Beachten Sie: Wenn angehängte Archive von der Untersuchung ausgeschlossen werden, hat das keinen Einfluss auf die Untersuchung von selbstextrahierenden Archiven. Diese werden immer auf allen Gliederungsstufen untersucht.
- **Angehängte Mail-Datenbanken untersuchen** – Untersuchung von in eine Nachricht eingebetteten Mail-Datenbanken.

Im Abschnitt **Einstellungen für Ports** können Sie die Werte der Mail-Ports POP3 und SMTP definieren, auf denen die Datenübertragung stattfindet. Als Standard gelten die Ports 110 und 25. Wenn Ihr Mailprogramm andere Ports verwendet, müssen deren Werte angegeben werden.

Erweitertkönnen die Untersuchungszeit und die Größe eines zu untersuchenden Objekts begrenzt werden:

- **Nicht untersuchen, wenn Nachricht größer als (MB)**, um die Größe von zu untersuchenden Objekten zu begrenzen; legen Sie die maximale Größe eines zu untersuchendes Objekts fest (in MB).
- **Beenden, wenn Untersuchung länger dauert als (Sek.)** zur Zeitbegrenzung der Untersuchung eines Objekts; legen Sie für das Untersuchungsintervall einen Wert (in Sekunden) fest.

Im Abschnitt **Beschleunigung der Objektuntersuchung** können Sie die Verwendung der Technologie iChecker™ zur Beschleunigung der Antiviren-untersuchung aktivieren/deaktivieren. Aktivieren Sie das Kontrollkästchen **iChecker™-Technologie verwenden**, damit die Technologie verwendet wird.

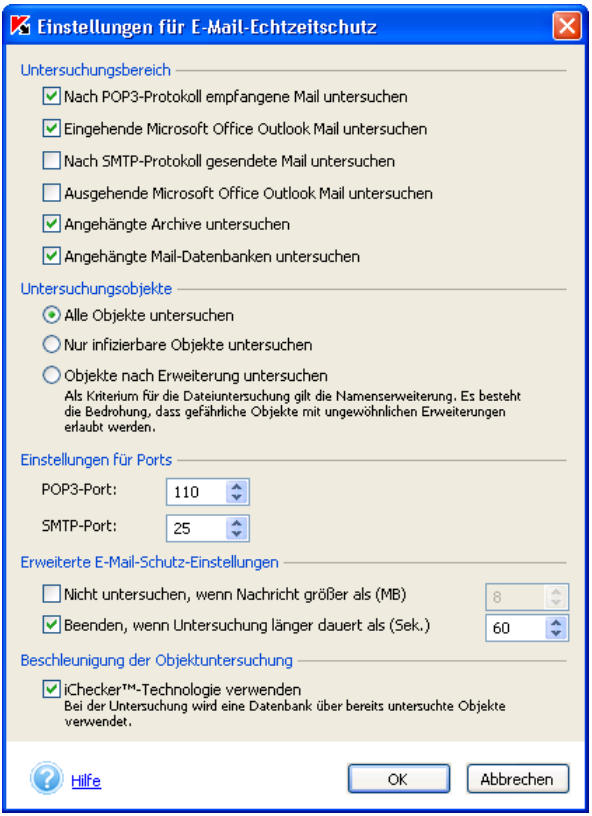
Einstellungen für E-Mail-Echtzeitschutz
Untersuchungsbereich
Nach POP3-Protokoll empfangene Mail untersuchen
Eingehende Microsoft Office Outlook Mail untersuchen
Nach SMTP-Protokoll gesendete Mail untersuchen
Ausgehende Microsoft Office Outlook Mail untersuchen
Angehängte Archive untersuchen
Angehängte Mail-Datenbanken untersuchen
Untersuchungsobjekte
Alle Objekte untersuchen
Nur infizierbare Objekte untersuchen
Objekte nach Erweiterung untersuchen
Als Kriterium für die Dateiuntersuchung gilt die Namenserweiterung. Es besteht die Bedrohung, dass gefährliche Objekte mit ungewöhnlichen Erweiterungen erlaubt werden.
Einstellungen für Ports
POP3-Port: 110
SMTP-Port: 25
Erweiterte E-Mail-Schutz-Einstellungen
Nicht untersuchen, wenn Nachricht größer als (MB) 8
Beenden, wenn Untersuchung länger dauert als (Sek.) 60
Beschleunigung der Objektuntersuchung
iChecker™-Technologie verwenden
Bei der Untersuchung wird eine Datenbank über bereits untersuchte Objekte verwendet.
Hilfe
OK
Abbrechen

Abbildung 19. Detaillierte Einstellungen für den E-Mail-Echtzeitschutz

5.2.2.2. Auswahl der Aktion für gefundene Objekte

Wählen Sie im Abschnitt **Aktionen für erkanntes Objekt** (s. Abbildung 18) den Typ der Aktion aus, die beim Fund eines infizierten oder verdächtigen Objektes ausgeführt werden soll:

- *Reparieren; irreparable Objekte löschen* – Das infizierte Objekt wird repariert; wenn das Objekt nicht repariert werden kann, wird es gelöscht.
- *In Quarantäne speichern* – Das verdächtige Objekt wird in die Quarantäne zur weiteren Untersuchung mit Nutzung der aktualisierten Antiviren-Datenbanken, zur Wiederherstellung, zum Einschicken an Kaspersky Lab oder zum Löschen verschoben.

- *Löschen* – Das infizierte bzw. verdächtige Objekt wird gelöscht. Sollten Sie diese Aktion für das Objekt gewählt haben, wird eine Kopie angelegt und dann in das Backup verschoben. Sie können diese Kopie dann zur Wiederherstellung der Datei oder zum Einschicken an Kaspersky Lab nutzen.

5.2.3. Untersuchung der E-Mails in Microsoft Office Outlook

Die Untersuchung von E-Mails in Microsoft Office Outlook geschieht mithilfe eines gesondertes Moduls, das in Microsoft Office Outlook integriert wird. Dieses Modul dient zur Untersuchung aller eingehenden E-Mails (Nachrichten und angehängte Dateien) vor dem Lesen sowie der ausgehenden E-Mails vor dem Senden.

Um das Untersuchungsfenster für E-Mails im Hauptmenü von Microsoft Office Outlook zu öffnen, wählen Sie den Menüpunkt **Extras** → **Optionen**. Im Fenster **Optionen** wechseln Sie in die Registerkarte **Kaspersky Anti-Virus** (s. Abbildung 20).

Im Abschnitt **Status** wird die Statusinformation über den Zustand des Moduls für die Mailuntersuchung angezeigt. Abhängig vom Status sind folgende Anzeigen möglich:

- *Die E-Mail-Untersuchung ist aktiviert*. Dieser Hinweis erscheint, wenn Kaspersky Anti-Virus gestartet wurde und die Untersuchung von E-Mails für Microsoft Office Outlook aktiviert ist.
- *Die Untersuchung von eingehender Mail ist aktiviert*. Dieser Hinweis erscheint, wenn nur die Untersuchung von ausgehender Mail aktiviert ist.
- *Die Untersuchung von ausgehender Mail ist aktiviert*. Dieser Hinweis erscheint, wenn nur die Untersuchung von ausgehenden Nachrichten aktiviert ist.
- *Die E-Mail-Untersuchung ist deaktiviert*. Dieser Hinweis erscheint, wenn die Untersuchung von eingehender und ausgehender Microsoft Office Outlook Mail deaktiviert ist und wenn Kaspersky Anti-Virus nicht gestartet wurde.

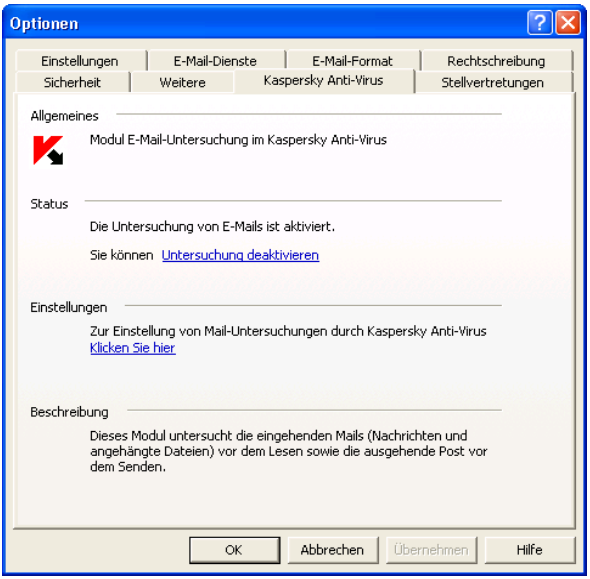

Abbildung 20. Registerkarte von Kaspersky Anti-Virus in Microsoft Office Outlook

Um die E-Mail-Untersuchung einzustellen, verwenden Sie den Hyperlink Klicken Sie hier im Abschnitt **Einstellungen**. Dadurch wird das Fenster mit den Einstellungen für den Echtzeitschutzes auf der Registerkarte **E-Mail** geöffnet (s. Abbildung 18).

Das Fenster mit den Echtzeitschutz-Einstellungen wird nur dann geöffnet, wenn im Fenster mit den erweiterten Einstellungen für Kaspersky Anti-Virus auf der Registerkarte **Allgemein** (s. Abb. 76) das Kontrollkästchen **Benutzeroberfläche anzeigen** aktiviert ist.

Für den Benutzer der Workstation wird auf der Registerkarte **Kaspersky Anti-Virus** (s. Abbildung 20) nur der Status **E-Mail-Untersuchung aktiviert/deaktiviert** angezeigt. Der Bereich Einstellungen ist inaktiv.

5.2.4. Untersuchung von Makros

Wenn die Makrountersuchung installiert und aktiviert ist, analysiert Kaspersky Anti-Virus im Echtzeitschutzmodus eine vom Programm vordefinierte Auswahl von VBA-Makrobefehlen und verhindert das Ausführen von schädlichem Code.

Die Einstellungen für die Makrountersuchung werden im Fenster **Echtzeitschutz-Einstellungen** auf der Registerkarte **Makros** (s. Abbildung 21) angepasst.

Die Makrountersuchung ist standardmäßig aktiviert. Um die Untersuchung abzuschalten, deaktivieren Sie das Kontrollkästchen **VBA-Makrountersuchung aktivieren**.

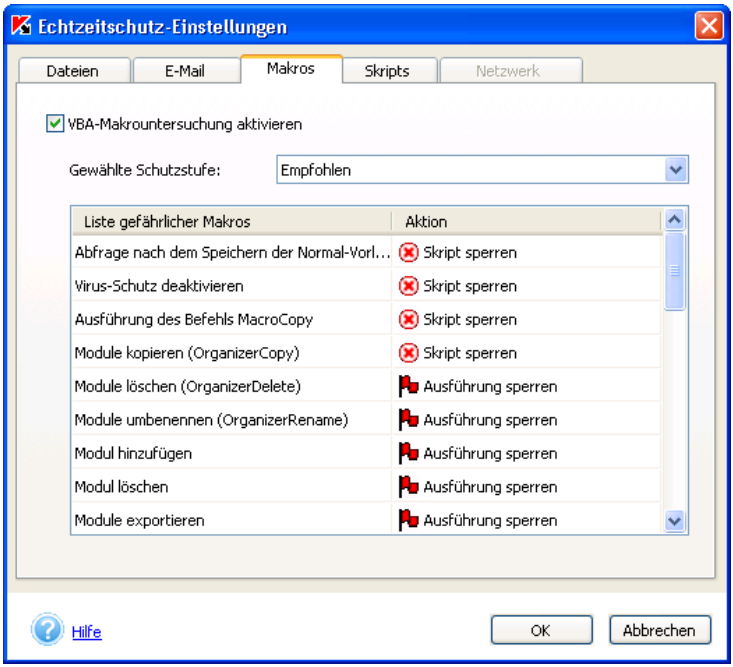

Abbildung 21. Optionen der Aufgabe zur Makrountersuchung

Wählen Sie in der Dropdown-Liste **Gewählte Schutzstufe** eine der drei von Kaspersky-Lab-Experten vordefinierten Stufen (Details s. Kapitel 4 auf S. 38).

Die Liste enthält die verdächtigen Makrobefehle, deren Arbeit vom Programm verfolgt wird, und eine der gewählten Sicherheitsstufe entsprechende Aktion für jeden Befehl.

Ausführung erlauben – Ausführung des Makrobefehls zulassen, keine Aktionen ausführen.

Aktion erfragen – Eine Eingabeaufforderung für die Aktion auf dem Bildschirm anzeigen. In dieser Anfrage werden alle für das betroffene Makro möglichen Aktionen aufgezählt.

Ausführung sperren – Ausführung des Makrobefehls sperren.

Skript sperren – Ausführung des Skripts, welches auf den Makrobefehl zugreifen wollte, beenden.

Sie können auf der Basis jeder Sicherheitsstufe eigene Einstellungen vornehmen. Dabei ändert sich die Sicherheitsstufe in **Benutzerdefinierte Einstellungen**. Bei der Rückkehr zu einer der drei vordefinierten Stufen werden die benutzerdefinierten Einstellungen nicht gespeichert.

Um die Aktion zu ändern, die Kaspersky Anti-Virus beim Fund eines verdächtigen Makrobefehls ausführen soll,

wählen Sie in der Tabelle die dem Makrobefehl entsprechende Zelle in der Spalte **Aktion** und wählen Sie aus der Dropdown-Liste eine der oben genannten Aktionen.

5.2.5. Skriptuntersuchung

Der Schutz Ihres Computers vor gefährlichen Skripts wird nur dann gewährleistet, wenn Sie seine Verwendung bei der Programminstallation nicht abgelehnt haben.

Wenn der Skript-Echtzeitschutz aktiviert ist, analysiert Kaspersky Anti-Virus im Echtzeitschutzmodus alle VBScript- und JavaScript-Skripts, bevor diese vom Skriptbearbeitungsmodul des Betriebssystems ausgeführt werden, und verhindert das Ausführen von schädlichem Code.

Die Skriptuntersuchung wird auf der Registerkarte **Skripts** des Dialogfensters **Echtzeitschutz-Einstellungen** (s. Abbildung 29) angepasst.

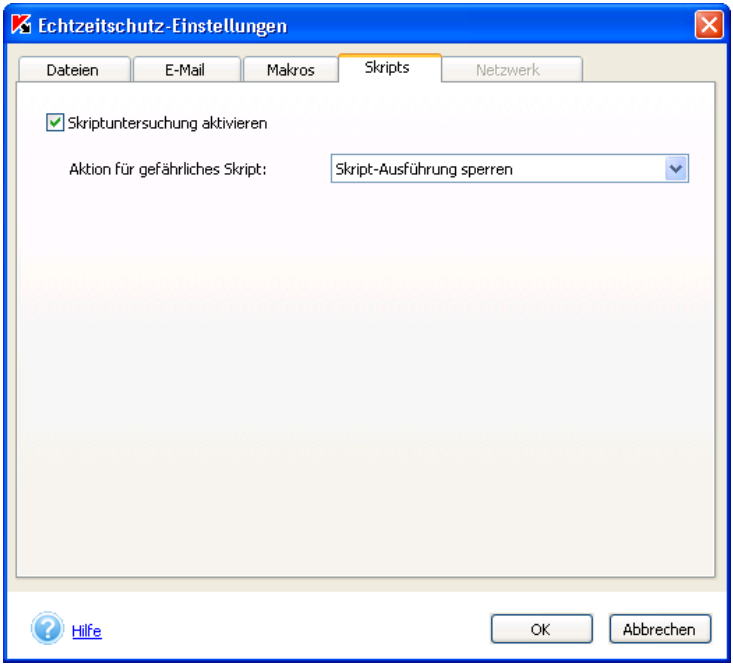

Abbildung 22. Parameter der Aufgabe zur Skriptuntersuchung

Die Skriptuntersuchung ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen **Skriptuntersuchung aktivieren**, um diese Untersuchung auszuschalten.

Geben Sie darunter die Aktion an, welche Kaspersky Anti-Virus beim Fund eines gefährlichen Skripts ausführen soll:

- **Benutzer nach Aktion fragen** – Eine Meldung über den Fund des potentiell gefährlichen Skripts auf dem Bildschirm anzeigen und den Benutzer nach weiteren Aktionen fragen. In dieser Anfrage werden alle Aktionen aufgezählt, die zur Verfügung stehen.
- **Skript-Ausführung sperren** – Den Start des Skripts sperren.
- **Skript-Ausführung erlauben** – Den Start des Skripts zulassen.

Während der Untersuchung von Skripts wird in der Statuszeile der Anwendung Microsoft Internet Explorer das blinkende Symbol von Kaspersky Anti-Virus eingeblendet.

5.2.6. Schutz vor Netzwerk-Angriffen

Der Schutz Ihres Computers vor Netzwerkangriffen wird nur dann gewährleistet, wenn Sie bei der Programminstallation seine Verwendung nicht abgelehnt haben.

Kaspersky Anti-Virus erlaubt den Schutz Ihres Computers vor Netzwerk-Angriffen durch Hacker aus dem lokalen Netzwerk oder Internet.

Die Analyse von Hacker-Angriffen wird auf Basis von Datenbanken der momentan bekannten Angriffe ausgeführt. Diese Datenbanken werden gemeinsam mit den Antiviren-Datenbanken aktualisiert und installiert (Details s. Pkt. 5.1 auf S. 43).

Der Schutz vor Netzwerk-Angriffen wird beim Start von Kaspersky Anti-Virus gestartet und untersucht alle über ein Netzwerk empfangenen Daten unabhängig von deren Quelle (lokales Netzwerk oder Internet).

Sobald auf Ihren Computer ein Angriffsversuch erfolgt, wird er blockiert. Auf dem Bildschirm erscheint eine entsprechende Meldung (s. Abbildung 23), die über die Art des Angriffs, die IP-Adresse des angreifenden Computers und den lokalen Port (falls möglich) informiert.

Der Echtzeitschutz vor Netzwerk-Angriffen wird auf der Registerkarte **Netzwerk** des Dialogfensters **Echtzeitschutz-Einstellungen** (s. Abbildung 24) angepasst.

Beim Deaktivieren/Aktivieren des Echtzeitschutzes aus dem Kontextmenü von Kaspersky Anti-Virus in der Taskleiste wird auch der Schutz vor Netzwerk-Angriffen abgeschaltet/aktiviert (s. Pkt. 5.2 auf S. 56).

Wenn Sie nur den Schutz vor Netzwerk-Angriffen abschalten möchten, ohne die anderen Echtzeitschutz-Aufgaben abzuschalten, deaktivieren Sie das Kontrollkästchen **Schutz vor Netzwerk-Angriffen aktivieren** (s. Abbildung 24). Beim Aktivieren/ Deaktivieren des Schutzes ist der Neustart des Computers erforderlich.

Kaspersky Anti-Virus for Windows Workstations
Achtung! Ihr Computer wurde aus dem Internet angegriffen.
Der Netzangriff ICMP Flood von der Adresse 10.0.0.1 wurde erfolgreich abgewehrt.
Diesen Hinweis während dieser Sitzung nicht mehr anzeigen
Hilfe
Tonsignale AUS
OK

Abbildung 23. Meldung über einen Netzwerk-Angriff

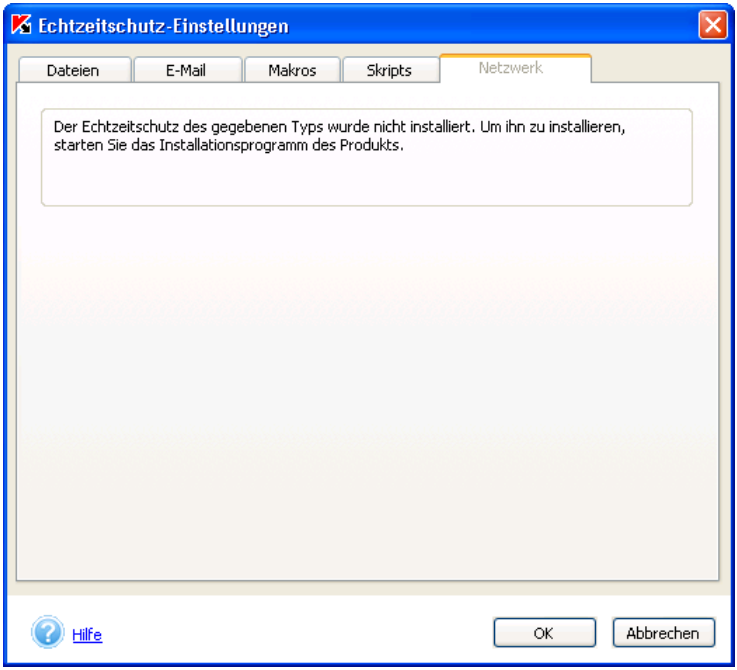

Abbildung 24. Echtzeitschutz vor Netzwerk-Angriffen anpassen

Für den Netzwerk-Echtzeitschutz stehen folgende Optionen von Kaspersky Anti-Virus zur Verfügung:

- **Stealth-Modus**. In diesem Modus wird nur die vom Benutzer oder von auf dem Computer installierten Programmen initiierte Netzwerk-Aktivität erlaubt. Jede andere Aktivität (entfernter Verbindungsaufbau mit Ihrem Computer usw.) wird verboten. Praktisch bedeutet dies, dass Ihr Computer für die externe Umgebung "unsichtbar" wird. Außerdem erlaubt der Stealth-Modus die Abwehr aller Angriffe des Typs DoS (Denial of Service). Dabei übt der Tarnmodus keinen negativen Einfluss auf Ihre Arbeit im Internet aus: Kaspersky Anti-Virus erlaubt die von Ihnen initiierte Netzwerk-Aktivität.

  Achtung! Der Stealth-Modus schützt Ihren Computer nicht vor den Aktionen Trojanischer Programme!

  Der Tarnmodus ist standardmäßig deaktiviert. Um ihn zu aktivieren, aktivieren Sie das Kontrollkästchen **Stealth-Modus verwenden**.

- **Benachrichtigung über Netzwerk-Angriffe**. In der Grundeinstellung werden Sie vom Programm über jeden Angriffsversuch auf Ihren Computer informiert. Dazu erscheint eine Meldung (s. Abbildung 23) auf dem Bildschirm, die Informationen darüber enthält, welcher Angriff erfolgte, von welcher IP-Adresse und auf welchem Port er ausgeführt wurde (falls diese Angaben ermittelt werden konnten). Da diese Meldung rein informativen Charakter besitzt, kann die Anzeige deaktiviert werden, wozu das Kontrollkästchen **Benutzer über Netzwerk-Angriffe informieren** dient, wobei Informationen über Angriffe trotzdem protokolliert werden.

- **Blockieren des angreifenden Computers**. Kaspersky Anti-Virus kann alle Computer sperren, von denen aus versucht wird, Ihren Computer anzugreifen. Das Blockieren des angreifenden Computers ist nicht standardmäßig aktiviert. Wenn Sie diesen Modus aktivieren, beträgt die standardmäßige Zeit für das Blockieren 60 Minuten. Während diesem Zeitraum werden alle Pakete, die vom angreifenden Computer an Ihren Computer gesendet werden, blockiert. Um den Blockierzeitraum zu ändern, geben Sie einen entsprechenden Wert für den Parameter **Angreifenden Computer für (Min.) sperren** an. Um den Blockier-Modus abzuschalten, deaktivieren Sie das Kontrollkästchen neben diesem Parameter.

5.3. Scan auf Befehl

Analyse von Objekten auf Befehl – Dieser Modus sieht eine Untersuchung des Computers auf das Vorhandensein von schädlichem Code auf Befehl des

Systemadministrators oder Benutzers der Workstation sowie eine Reparatur und Löschung von infizierten Objekten und Verschieben von verdächtigen Objekten in Quarantäne vor.

Kaspersky Anti-Virus erlaubt die vollständige Untersuchung des gesamten Computers oder die Untersuchung ausgewählter Bereiche (einzelne Laufwerke, Ordner, Dateien, E-Mail). Dabei werden gefundene gefährliche Objekte desinfiziert oder gelöscht und verdächtige Objekte in die Quarantäne verschoben.

Bei der Installation der Anwendung werden standardmäßig Systemaufgaben für den Scan auf Befehl erstellt:

- **Arbeitsplatz untersuchen** – vollständige Untersuchung des gesamten Dateisystems des Computers (s. Pkt. 5.3.1 auf S. 78); wird standardmäßig automatisch jeden Freitag um 20:00 Uhr gestartet.
- **Wechseldatenträger untersuchen** – Untersuchung von Wechseldatenträgern (Disketten, CD-ROMs, Flash-Cards usw.); wird standardmäßig manuell vom Benutzer gestartet (s. Pkt. 5.3.5 auf S. 93).
- **Kritische Bereiche untersuchen** – Untersuchung des Systemspeichers, der Autostart-Objekte, Laufwerksbootsektoren sowie der Systemordner *Windows* und *Windows/system32*; wird standardmäßig manuell vom Benutzer gestartet.
- **Quarantäne untersuchen** – Untersuchung der Objekte, die in der Quarantäne gespeichert wurden; wird standardmäßig manuell vom Benutzer gestartet.
- **Untersuchung bei Start von Kaspersky Anti-Virus** – Untersuchung von Autostart-Objekten, Systemspeicher und Bootsektoren; wird standardmäßig automatisch beim Start des Betriebssystems Ihres Computers gestartet.

Außerdem ist die Möglichkeit zur Untersuchung eines Objekts, das vom Benutzer festgelegt wird, vorgesehen (Details s. Pkt. 5.3.2 auf S. 79). Daneben können Sie selbständig zusätzliche Aufgaben zur Untersuchung von Objekten auf Befehl erstellen (s. Pkt. 5.6 auf S. 101).

Um Mail-Datenbanken für Microsoft Outlook Express erfolgreich zu desinfizieren, muss vor der Untersuchung die Arbeit der Anwendung Microsoft Outlook Express beendet werden.

5.3.1. Vollständige Untersuchung des Computers

Die vollständige Untersuchung erlaubt es, eine größere Anzahl von Objekten auf Ihrem Computer zu überprüfen, als dies im Echtzeitschutz möglich ist. Deshalb wird empfohlen, die vollständige Untersuchung aus prophylaktischen Gründen mindestens einmal pro Woche auszuführen.

Das Programm informiert Sie darüber, wann der Start erforderlich ist. Falls das Programmhauptfenster geschlossen ist, erscheint über dem Symbol von Kaspersky Anti-Virus im Infobereich der Taskleiste ein kurzer Hinweis mit der Empfehlung, die Untersuchung zu starten (wenn die Option zur Anzeige von Popup-Informationen aktiviert ist s. Pkt. 5.10.4 auf S. 125).

Um ausführliche Informationen zu erhalten, öffnen Sie das Programmhauptfenster auf der Registerkarte **Sicherheit** (s. Abbildung 2) und überprüfen Sie den Status der vollständigen Untersuchung auf der rechten Seite des Fensters. Für die vollständige Untersuchung sind folgende Status möglich:

Die Untersuchung wird regelmäßig oder im Moment ausgeführt.

Der Start der Untersuchung ist erforderlich, wobei vorher die von Kaspersky-Lab-Experten empfohlenen Einstellungen wiederhergestellt werden sollten.

Die sofortige vollständige Untersuchung des Computers ist erforderlich.

Bei Bedarf können Sie die Untersuchung direkt aus dem Statusbereich für die vollständige Untersuchung starten, indem Sie den Hyperlink vollständige Untersuchung verwenden.

Die Kaspersky-Lab-Experten empfehlen, den Modus zum zeitgesteuerten Start der vollständigen Untersuchung zu aktivieren. Der Status der vollständigen Untersuchung enthält Informationen darüber, ob dieser Modus aktiviert oder deaktiviert ist.

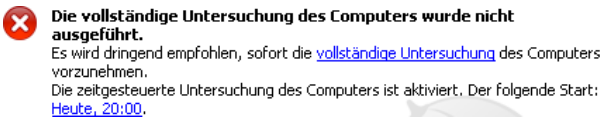
Die vollständige Untersuchung des Computers wurde nicht ausgeführt.
Es wird dringend empfohlen, sofort die vollständige Untersuchung des Computers vorzunehmen.
Die zeitgesteuerte Untersuchung des Computers ist aktiviert. Der folgende Start:
Heute, 20:00.

Abbildung 25. Informationen über die Aktualität der Untersuchung

*Um den Computer auf Befehl zu scannen, wählen Sie im linken Teil der Registerkarte **Sicherheit**:*

Arbeitsplatz untersuchen – Start der vollständigen Virensuche im Computer entsprechend der gewählten Einstellungen (s. unten). Eine analoge Aktion wird mit dem Hyperlink Vollständige Untersuchung ausführen im rechten Teil der Registerkarte **Sicherheit** ausgeführt sowie mit dem Menüpunkt **Arbeitsplatz auf Viren untersuchen** im Kontextmenü, das sich durch Rechtsklick auf das Programmsymbol in der Taskleiste öffnet.

Danach erscheint auf dem Bildschirm das Fenster **Untersuchung** (s. Abbildung 5). Dieses Fenster informiert mit Prozentangabe über die Ausführung des Untersuchungsprozesses. Es enthält außerdem den Namen des momentan untersuchten Objekts, die voraussichtliche Abschlusszeit der Untersuchung sowie eine Gesamtstatistik über die bisher untersuchten, desinfizierten, gelöschten und in die Quarantäne verschobenen Objekte.

Bei der vollständigen Untersuchung des Computers erfolgt keine Analyse von Mailboxen, Wechseldatenträgern und Netzlaufwerken, wenn solche an Ihren Computer angeschlossen sind.

Das Untersuchungsfenster kann ausgeblendet werden. Klicken Sie dazu auf die Schaltfläche in der rechten oberen Ecke und wählen Sie im folgenden Fenster die Variante **Fenster schließen, Untersuchung fortsetzen**.

Die Untersuchungsergebnisse können im aufgezeichneten Protokoll gelesen werden (Details s. Pkt. 5.10.2 auf S. 118).

5.3.2. Untersuchung eines ausgewählten Objekts

Ein Objekt kann entweder mit Hilfe der Oberfläche von Kaspersky Anti-Virus zur Untersuchung ausgewählte werden oder mit den Standardmitteln des Betriebssystems Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.).

Um ein Untersuchungsobjekt mit Hilfe von Kaspersky Anti-Virus auszuwählen,

verwenden Sie den Hyperlink Objekte untersuchen auf der linken Seite der Registerkarte **Sicherheit** (s. Abbildung 2).

Das folgende Fenster **Untersuchungsobjekte wählen** (s. Abbildung 26) enthält eine Liste der Objekte, die untersucht werden können, sowie Schaltflächen zum Ändern der Liste und zum Steuern der Untersuchung.

Standardmäßig enthält die Liste folgende Objekte:

- Wechseldatenträger (einschließlich Disketten und CD-ROM)
- Festplatten
- Netzlaufwerke (wenn diese an ihren Computer angeschlossen sind)
- Mailboxen für Microsoft Office Outlook und Microsoft Outlook Express
- Ordner **Eigene Dateien**
- Systemspeicher
- Autostart-Objekte
- Laufwerksbootsektoren

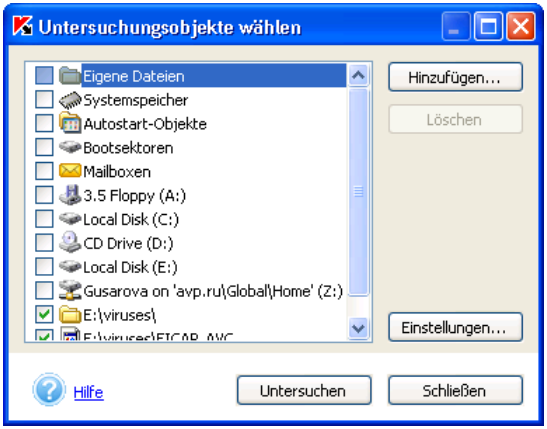

Abbildung 26. Auswahl der zu untersuchenden Objekte

Wenn Sie der Liste ein neues Objekt hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie im folgenden Fenster die gewünschte Datei oder den Ordner an. Alle Objekte, die Sie der Liste hinzufügen, werden darin auch für künftige Untersuchungen gespeichert.

Bei der Angabe des Pfads für einen Ordner oder ein Objekte können Sie Systemumgebungsvariable verwenden. Für die Untersuchung des Installationsordners des Betriebssystems Microsoft Windows können Sie beispielsweise die Variable **%windir%** verwenden.

Um ein Objekt aus der Liste zu entfernen, wählen Sie das Objekt aus und klicken Sie auf **Löschen**. Beachten Sie, dass nur jene Objekte aus der Liste entfernt werden können, die manuell hinzugefügt wurden. Objekte, die standardmäßig in der Liste enthalten sind, können nicht entfernt werden.

Wenn Sie die Parameter für die Untersuchung von ausgewählten Objekten ändern möchten, verwenden Sie die Schaltfläche **Einstellungen** (Details s. Pkt. 5.3.3 auf S. 82). Die vorgenommenen Änderungen werden für folgende Untersuchungen von Objekten der erstellten Liste sowie für die Untersuchung von Objekten, die mit Microsoft Windows-Mitteln ausgewählt werden, gespeichert.

Um bestimmte Objekte der Liste zu untersuchen,

1. Wählen Sie die Objekte aus der Liste aus.
2. Klicken Sie auf die Schaltfläche **Untersuchen**, um die Untersuchung zu starten.

Zum Starten der Untersuchung eines Objekts, das mit Microsoft Windows-Mitteln ausgewählt wurde,

führen Sie den Mauszeiger auf den Namen des gewählten Objekts, öffnen Sie durch Rechtsklick das Microsoft Windows-Kontextmenü und wählen Sie den Punkt **Auf Viren untersuchen** (s. Abbildung 27). Bei der Untersuchung werden die Einstellungen verwendet, die im Fenster **Untersuchungsobjekte wählen** (s. Abbildung 26) angegeben sind.

Abbildung 27. Virenuntersuchung eines mit Microsoft Windows-Mitteln ausgewählten Objekts

Wenn Kaspersky Anti-Virus nicht gestartet wurde, dann wird Ihnen vorgeschlagen ihn zu starten, wenn Sie die Untersuchung eines mit Windows-Mitteln ausgewählten Objekts aufrufen.

Unabhängig davon, mit welcher Methode die Untersuchung eines Objekts gestartet wurde (aus dem Windows-Kontextmenü oder aus der Objektliste von Kaspersky Anti-Virus), wird auf dem Bildschirm das Fenster **Untersuchung** geöffnet (s. Abbildung 5). Die Untersuchungsergebnisse können im aufgezeichneten Protokoll gelesen werden (Details s. Pkt. 5.10.2 auf S. 118).

Wenn bestimmte Objekte regelmäßig untersucht werden sollen, können Sie eine entsprechende Aufgabe für den Scan auf Befehl erstellen (Details s. Pkt. 5.6 auf S. 101).

5.3.3. Einstellungen für Scan auf Befehl

Um die Einstellungen für den Scan auf Befehl anzuzeigen oder zu ändern:

Klicken Sie auf den Hyperlink Scan auf Befehl auf der linken Seite der Registerkarte **Einstellungen** (s. Abbildung 3).

Dadurch wird das Fenster **Scan auf Befehl** (s. Abbildung 28) geöffnet, das eine Liste der Systemaufgaben und der vom Benutzer erstellten Untersuchungsaufgaben enthält.

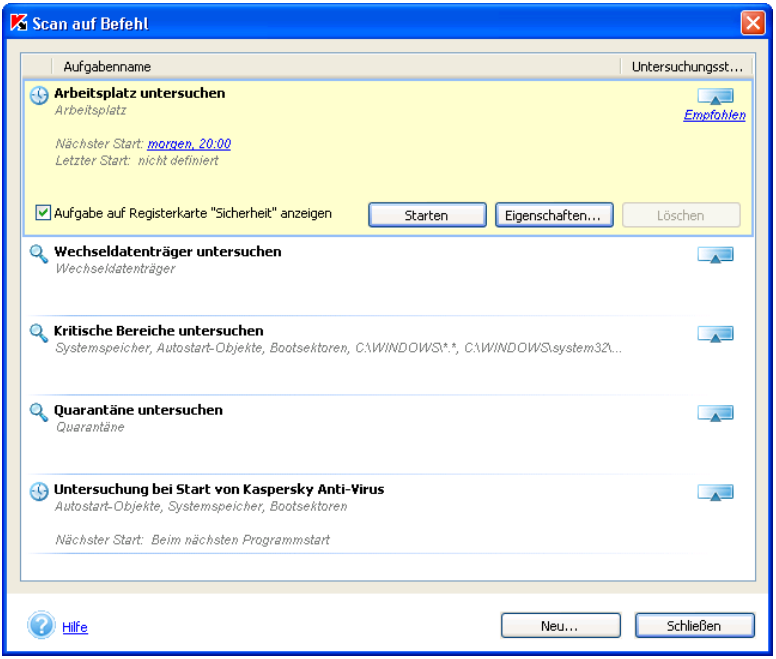

Abbildung 28. Liste der Aufgaben für Scan auf Befehl

Durch Mausklick auf den Namen einer Aufgabe wird ein Block geöffnet, der Informationen über den Untersuchungsbereich und die Zeit des nächsten und letzten Starts der Untersuchungsaufgabe enthält. In diesem Block können Sie den Scan auf Befehl mit der Schaltfläche **Starten** manuell starten. Mit der Schaltfläche **Eigenschaften** wird das Konfigurationsfenster der Untersuchungsaufgabe (s. Abbildung 29) geöffnet, in dem folgende Funktionen angepasst werden können:

- Untersuchungsobjekte auswählen. Die Auswahl ist möglich für Aufgaben, die manuell erstellt wurden. Um ein neues Objekt hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie in der Dropdown-Liste das gewünschte Objekt. Um ein Objekt, das nicht in der Liste vorhanden ist, zu untersuchen (beispielsweise einen bestimmten Ordner oder eine Datei), wählen Sie in der Liste die Zeile **Durchsuchen** und geben Sie den Pfad des Objekts an. Um ein Objekt aus der Untersuchungsliste zu löschen, wählen Sie es in der Liste aus und klicken Sie auf **Löschen**.

- die Antivirenschutzstufe festlegen und die gewählte Sicherheitsstufe detailliert anpassen (s. Pkt. 5.3.3.1 auf S. 85);

- eine Liste der Objekte erstellen, die von der Untersuchung ausgeschlossen werden sollen (s. Pkt. 5.7 auf S. 102). Verwenden Sie den Hyperlink nicht festgelegt/ festgelegt in der Beschreibung der geltenden Schutzeinstellungen, um in das Fenster zum Erstellen der Ausnahmenliste zu gelangen. Das Aussehen des Hyperlinks ist davon abhängig, ob Ausnahmen festgelegt sind oder nicht.

- die Aktion festlegen, die von Kaspersky Anti-Virus beim Fund gefährlicher und verdächtiger Objekte angewandt werden soll (s. Pkt. 5.3.3.2 auf S. 88).

- einen Zeitplan für den automatischen Start von Untersuchungsaufgaben erstellen (s. Pkt. 5.8 auf S. 106);

- den Start einer Aufgabe mit den Rechten eines anderen Benutzers anpassen (nur für Computer mit dem Betriebssystem Microsoft Windows NT/2K/XP) (s. Pkt. 5.9 auf S. 110).

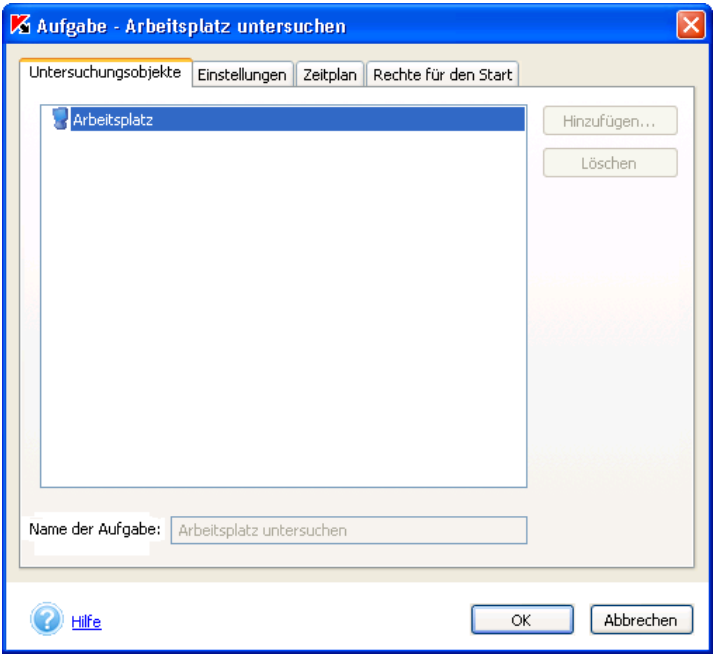

Abbildung 29. Konfigurationsfenster für Scan auf Befehl.
Registerkarte **Untersuchungsobjekte**

Wenn Sie planen, die Aufgabe häufig zu starten, wird empfohlen, im Infoblock der Aufgabe das Kontrollkästchen **Aufgabe auf Registerkarte "Sicherheit" anzeigen** zu aktivieren. Dadurch können Sie die Aufgabe schnell über einen gleichnamigen Hyperlink starten, der sich auf der linken Seite der Registerkarte **Sicherheit** (s. Abbildung 2) befindet.

Links vom Namen der Aufgabe können abhängig von der Situation folgende Symbole angezeigt werden:

– Für diese Aufgabe wurde ein Zeitplan erstellt, nach dem sie automatisch ausgeführt wird.

– Diese Aufgabe wird im Moment ausgeführt.

Um eine neue Untersuchungsaufgabe zu erstellen, verwenden Sie die Schaltfläche **Neu** im Fenster **Scan auf Befehl** (s. Abbildung 28). Details zum Erstellen einer Aufgabe s. Pkt. 5.6 auf S. 101.

Um eine Aufgabe zu löschen, wählen Sie diese in der der Liste aus und klicken Sie auf **Löschen**. Beachten Sie dabei, dass nur jene Aufgaben aus der Liste

gelöscht werden können, die manuell hinzugefügt worden sind. Systemaufgaben können nicht entfernt werden. Auch Aufgaben, die gerade ausgeführt werden, können nicht entfernt werden.

5.3.3.1. Auswahl der Untersuchungsstufe

Wählen Sie auf der Registerkarte Einstellungen (s. Abbildung 30) in der Dropdown-Liste **Gewählte Schutzstufe** eine der drei von Kaspersky-Lab-Experten vordefinierten Stufen (Details s. Kapitel 4 auf S. 38). Standardmäßig gelten die Einstellungen der empfohlenen Sicherheitsstufe.

Sie können auf der Basis jeder Sicherheitsstufe eigene Einstellungen vornehmen. Dabei ändert sich die Sicherheitsstufe in **Benutzerdefinierte Einstellungen**. Bei der Rückkehr zu einer der drei vordefinierten Stufen werden die benutzerdefinierten Einstellungen nicht gespeichert.

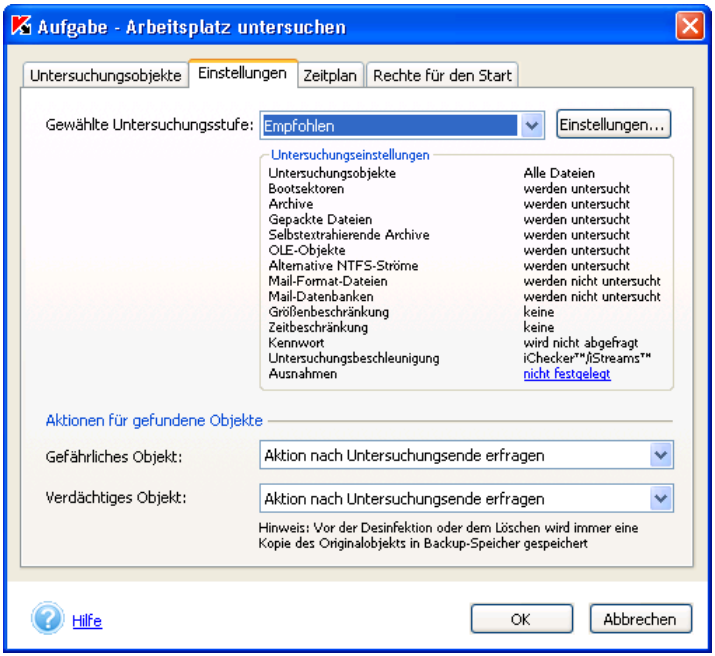

Abbildung 30. Einstellungen für Scan auf Befehl

Die Einstellungen der gewählten Stufe können im Fenster **Einstellungen für Scan auf Befehl** (s. Abbildung 31) überprüft und geändert werden. Dieses Fenster wird mit der Schaltfläche **Einstellungen** geöffnet (s. Abbildung 30).

Wählen Sie im Abschnitt **Untersuchungsobjekte** die Objekte, welche von Kaspersky Anti-Virus untersucht werden sollen:

- **Alle Objekte untersuchen** – Dateien untersuchen, ohne Berücksichtigung des Typs und der Erweiterung.
- **Nur infizierbare Objekte untersuchen** – Dateien untersuchen, deren Infektion potentiell möglich ist; die Analyse der Infizierbarkeit basiert auf der internen Dateistruktur.
- **Objekte nach Erweiterung untersuchen** – Dateien untersuchen, die potentiell infiziert werden können; die Analyse der Infizierbarkeit basiert auf der Dateinamenserweiterung.

Im Abschnitt **Erweiterte Untersuchungseinstellungen** können Sie festlegen, ob folgende Objekte untersucht werden sollen:

- Laufwerksbootsektoren
- Archive
- gepackte ausführbare Dateien
- selbstextrahierende Archive
- angehängte oder in andere Dateien eingebettete Objekte (*OLE-Objekte*)
- alternative NTFS-Ströme
- Mail-Dateien
- Mail-Datenbanken

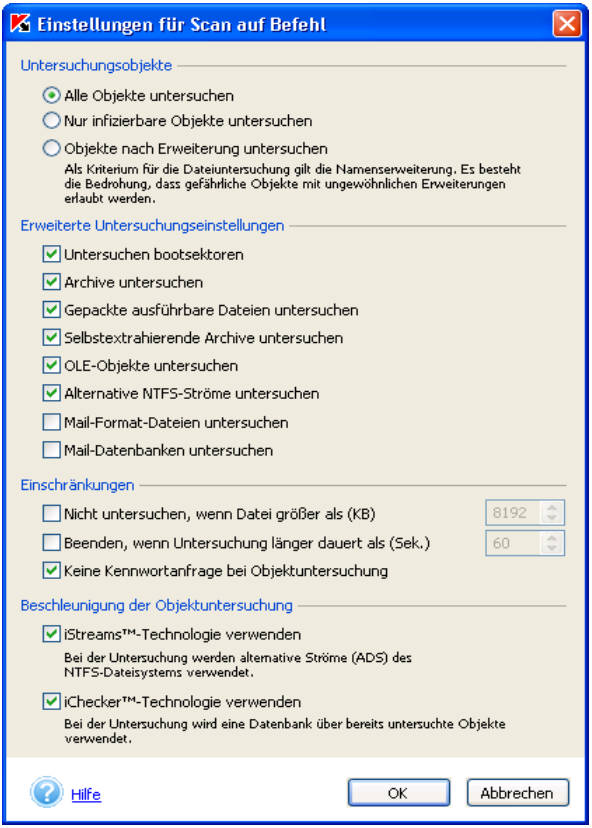

Abbildung 31. Detailliertes Anpassen von Scan auf Befehl

Aktivieren Sie im Abschnitt **Einschränkungen** die gewünschten Kontrollkästchen:

- **Nicht untersuchen, wenn Datei größer als (KB)**, um die Größe von zu untersuchenden Objekten zu begrenzen; legen Sie die maximale Größe eines zu untersuchendes Objekts (in KB) fest.
- **Beenden, wenn Untersuchung länger dauert als (Sek.)** zur Zeitbegrenzung der Untersuchung eines Objekts; legen Sie einen Wert für das Untersuchungsintervall (in Sekunden) fest.
- **Keine Kennwortabfrage bei Objektuntersuchung**, damit bei der Untersuchung von durch Kennwort geschützten Objekten keine Kennwortabfrage erfolgt. Wenn dieses Kontrollkästchen aktiviert ist,

werden kennwortgeschützte Objekte bei der Antivirenuntersuchung übersprungen.

Im Abschnitt **Beschleunigung der Objektuntersuchung** können Sie die Verwendung von Technologien iChecker™ und iStreams™ zur Beschleunigung der Antivirenuntersuchung aktivieren/deaktivieren. Aktivieren Sie die entsprechenden Kontrollkästchen, damit die Technologien verwendet werden.

Wenn Sie die Verwendung der Technologie iStreams™ bei der Programminstallation abgelehnt haben, ist die Neuinstallation von Kaspersky Anti-Virus erforderlich, um iStreams™ zu aktivieren. Erst danach stehen die Einstellungen für diese Technologie zur Verfügung.

5.3.3.2. Auswahl der Aktion für gefundene Objekte

In den Abschnitten **Aktionen für infizierte/verdächtige Objekte** (s. Abbildung 31) wählen Sie den Aktionstyp aus, die beim Auftreten solcher Objekte angewendet werden soll:

- **Aktion nach Untersuchungsende erfragen** – Nach Abschluss der Untersuchung wird die Bearbeitung der gefährlichen Objekte angeboten. Dieser Modus ist standardmäßig festgelegt und macht die ständige Anwesenheit des Benutzers am Computer überflüssig. Da eine Untersuchung relativ viel Zeit beanspruchen kann, erlaubt dieser Modus die Zeitersparnis bei der Arbeit mit Kaspersky Anti-Virus, wenn Ihnen die Kontrolle der Bearbeitung gefährlicher Objekte nicht im Moment des Funds möglich ist.
- **Aktion während Untersuchung erfragen** – Während der Untersuchung werden auf dem Bildschirm Anfragen nach den auszuführenden Aktionen für das Objekt angezeigt. Die Anfrage enthält alle für das Objekt möglichen Aktionen. Eine dieser Aktionen wird von Kaspersky-Lab-Experten empfohlen. Wählen Sie diesen Modus der Programmfunktion, wenn Sie sich während der Untersuchung am Computer aufhalten werden.
- **Empfohlene Aktion ausführen** – Die von Kaspersky-Lab-Experten empfohlene Aktion wird ausgeführt. Da die empfohlene Aktion immer begründet ist, können Sie diesen Modus in der Mehrzahl der Fälle wählen. Folgende Aktionen werden empfohlen:

- *Desinfizieren* des infizierten Objekts, *irreparable Objekte löschen*[6].
- *Nach Quarantäne verschieben*. Das Objekt, das möglicherweise von einem Virus oder dessen Modifikation infiziert ist, wird in die Quarantäne verschoben.

Es kann vorkommen, dass nach dem Verschieben einer Datei in die Quarantäne auf dem Bildschirm eine Meldung darüber erscheint, dass das Objekt nicht gelöscht werden kann. Der Grund liegt darin, dass Objekte beim Speichern in Quarantäne verschoben werden, d.h. sie werden nach Quarantäne kopiert und am ursprünglichen Speicherort gelöscht. Allerdings kann beim Verschieben nicht jedes Objekt gelöscht werden, z.B. ein Objekt, das momentan von einem anderen Programm verwendet wird.

- *Löschen* des gefährlichen Objekts, wenn es ein trojanisches Programm oder Wurm ist.

Wenn ein infiziertes / möglicherweise infiziertes Objekt als potentiell gefährliches Programm gilt, wird das Objekt *übersprungen*.

- **Desinfizieren, irreparable Objekte löschen** – Es wird versucht, das gefährliche Objekt zu desinfizieren. Wenn die Desinfektion nicht möglich ist, wird das Objekt gelöscht. In diesem Fall werden auch potentiell gefährliche Objekte der Desinfektion unterzogen und gelöscht, falls sie nicht desinfiziert werden können. Bei der Desinfektion wird eine Kopie des Objekts im Backup aufbewahrt.
- **Objekte löschen** – Ein bei der Untersuchung gefundenes gefährliches Objekt wird ohne Bestätigung des Benutzers und ohne Desinfektionsversuch gelöscht. Beim Löschen des Objekts wird eine Kopie im Backup-Speicher aufbewahrt. Dieser Funktionsmodus von Kaspersky Anti-Virus wird empfohlen, wenn Sie überzeugt sind, dass der Verlust wichtiger Informationen ausgeschlossen ist.
- **Informationen protokollieren** – Keine Aktionen mit dem Objekt vornehmen. Es werden nur Informationen über die Infektion im Protokoll über die Programmarbeit aufgezeichnet. Wir empfehlen, diesen Modus möglichst selten zu wählen, da gefährliche und andere schädliche Objekte auf Ihrem Computer verbleiben.

[6] Standardmäßig werden infizierte Objekte des Arbeitsspeichers gelöscht, wogegen vireninfizierte Bootsektoren der Desinfektion unterzogen und übersprungen werden, falls die Desinfektion nicht möglich ist.

Es kann vorkommen, dass das Ausführen einer Aktion mit einem Objekt nicht möglich ist. Die Bearbeitung eines infizierten Objekts ist z.B. nicht möglich, wenn es im Moment der Untersuchung von einer anderen Anwendung benutzt wird. In diesem Fall erscheint eine entsprechende Meldung auf dem Bildschirm (s. Abbildung 32), in der folgende Aktionen angeboten werden:

- *Desinfizieren bei Neustart des Computers*. Diese Aktion wird nur angeboten, wenn die Desinfektion des Objekts möglich ist.
- *Löschen bei Neustart des Computers*.
- *Überspringen* – Keine Aktionen mit dem Objekt vornehmen. Es werden nur Informationen über den Virusfund im Protokoll über die Programmarbeit aufgezeichnet.

  Wenn Sie die Meldung mit Hilfe der Schaltfläche in der rechten oberen Ecke schließen, wird die ausgewählte Aktion nicht ausgeführt und das Objekt wird übersprungen.

Kaspersky Anti-Virus for Windows Workstations
Achtung! Desinfektion des Objekts ist nicht möglich.
Objekt C:\...\eicar\eicar.com.cure kann nicht desinfiziert werden, weil kein Zugriffsrecht besteht oder Zugriff auf das Objekt nicht möglich ist. Wir empfehlen Desinfizieren bei Neustart des Computers.
Desinfizieren bei Neustart des Computers (empfohlen)
Löschen bei Neustart des Computers
Überspringen
Anwenden auf alle Objekte , die blockiert wurden (während dieser Sitzung)
Hilfe
Tonsignale AUS
OK

Abbildung 32. Die sofortige Desinfektion des Objekts ist nicht möglich

5.3.4. Untersuchung von Archiven

Kaspersky Anti-Virus untersucht Archive dann, wenn die Sicherheitsstufe **Maximale Sicherheit** oder **Empfohlen** gewählt wurde und die Untersuchung von Archiven nicht deaktiviert wurde (wenn das Kontrollkästchen **Archive untersuchen** im Fenster **Einstellungen für Scan auf Befehl** nicht deaktiviert wurde, s. Abbildung 31).

Kaspersky Anti-Virus untersucht alle Objekte innerhalb von Archiven, desinfiziert aber nur Objekte in Archiven der Typen *zip*, *arj*, *cab*, *rar*, *lha* und *ice*.

Kaspersky Anti-Virus desinfiziert selbstextrahierende Archive NICHT!

Wenn ein Archiv oder ein Objekt innerhalb eines Archivs durch Kennwort geschützt ist und der Modus zur Kennwortabfrage aktiviert ist, dann wird vor deren Untersuchung auf dem Bildschirm eine Anfrage nach dem Kennwort durchgeführt (s. Abbildung 33). Wenn der Modus zur aufgeschobenen Objektbearbeitung gewählt wurde (wenn in den Untersuchungseinstellungen die Aktion **Aktion nach Untersuchungsende erfragen** gewählt wurde, s. Pkt. 5.3.3.2 auf S. 88), dann erfolgt die Kennwortabfrage nach dem Abschluss der Untersuchung.

Die Anzeige der Kennwortabfrage wird durch das Kontrollkästchen **Keine Kennwortabfrage bei Untersuchung von Objekten** in den Untersuchungseinstellungen reguliert (s. Pkt. 5.3.3.1 auf S. 85). In der Grundeinstellung ist dieses Kontrollkästchen nur für die Stufe **Maximaler Schutz** deaktiviert.

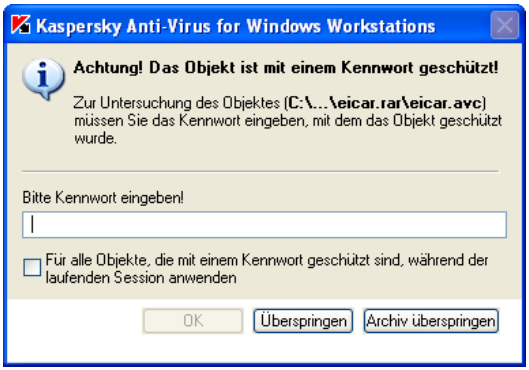
Kaspersky Anti-Virus for Windows Workstations
Achtung! Das Objekt ist mit einem Kennwort geschützt!
Zur Untersuchung des Objektes (C:\...\eicar.rar\eicar.avc) müssen Sie das Kennwort eingeben, mit dem das Objekt geschützt wurde.
Bitte Kennwort eingeben!
Für alle Objekte, die mit einem Kennwort geschützt sind, während der laufenden Session anwenden
OK
Überspringen
Archiv überspringen

Abbildung 33. Kennworteingabe für Archivuntersuchung

In das Feld **Kennwort** geben Sie das Kennwort für den Zugriff auf die Objekte des zu untersuchenden Archivs ein und klicken auf die Schaltfläche **OK**. Die Untersuchung des Archivs und ihm zugehörigen Objekte auf Virenbefall wird somit gestartet.

Bei der Bearbeitung (Desinfektion, Löschen) von Objekten in einem Archiv entpackt Kaspersky Anti-Virus das Archiv in einen temporären Ordner, untersucht, bearbeitet und verpackt seine Objekte unter dem gleichen Namen und kopiert das Archiv an den ursprünglichen Ort, wobei das dort vorhandene Archiv ersetzt wird. Für die Bearbeitung kennwortgeschützter Objekte in einem Archiv ist die gleiche Bearbeitungsprozedur vorgesehen. Eine Besonderheit besteht darin, dass die Objekte nach der Bearbeitung ohne Kennwort in ein Archiv verpackt werden.

Wird bei der Untersuchung ein anderes kennwortgeschütztes Objekt innerhalb eines Archivs gefunden, dann versucht Kaspersky Anti-Virus darauf das von Ihnen für das erste Objekt angegebene Kennwort anzuwenden. Nur wenn dieses Kennwort nicht zutrifft, wird auf dem Bildschirm erneut die Anfrage nach Kennworteingabe angezeigt.

Ist Ihnen das Kennwort unbekannt, dann ist die Untersuchung des geschützten Archivs und aller darin enthaltenen Objekte nicht möglich. Wir empfehlen, in diesem Fall auf die Schaltfläche **Überspringen** zu klicken und die Untersuchung fortzusetzen.

Klicken Sie auf die Schaltfläche **Archiv überspringen**, um von der laufenden Untersuchung alle kennwortgeschützten Objekte auszunehmen, die zu dem zu untersuchenden Archiv gehören. Dabei werden alle Objekte innerhalb eines Archivs, die nicht kennwortgeschützt sind, gemäß den Einstellungen für die Aufgabe untersucht und verarbeitet.

Das Kontrollkästchen **Für alle Objekte, die mit einem Kennwort geschützt sind, während der laufenden Session anwenden** bezieht sich auf die Aktion, die nach dem Aktivieren des Kontrollkästchens gewählt wird.

Wenn Sie beispielsweise bei aktiviertem Kontrollkästchen **Überspringen**, **Archiv überspringen** ausgewählt haben, dann werden die übrigen kennwortgeschützten Objekte nicht untersucht. Sollten Sie jedoch ein Kennwort eingegeben und auf **OK** geklickt haben, dann versucht das Programm, dieses Kennwort ohne weitere Dialogfenster auf alle übrigen kennwortgeschützten Objekte anzuwenden.

Wenn ein Archiv nicht desinfiziert werden kann und in den Untersuchungseinstellungen als Aktion beim Fund eines gefährlichen Objekts die Variante **Empfohlene Aktion ausführen** gewählt wurde, dann löscht Kaspersky Anti-Virus das Archiv nicht, sondern protokolliert nur Informationen über den Fund.

Wenn in den Untersuchungseinstellungen als Aktion die Varianten **Aktion nach Untersuchungsende erfragen** oder **Aktion während Untersuchung erfragen** (s. Pkt. 5.3.3.2 auf S. 88) gewählt wurde, können Sie das irreparable Archiv löschen. Wählen Sie dazu in der Eingabeaufforderung die Aktion **Löschen**. Außerdem können Sie das Archiv auch manuell löschen.

5.3.5. Untersuchung von Wechseldatenträgern

Die Untersuchung von Wechseldatenträgern kann aus dem Hauptfenster von Kaspersky Anti-Virus oder aus dem Microsoft Windows-Kontextmenü (aus dem Fenster des Programms **Explorer**, auf dem **Arbeitsplatz** usw.) gestartet werden.

Um die Untersuchung von Wechseldatenträgern aus dem Microsoft Windows-Kontextmenü zu starten,

wählen Sie die Laufwerke aus (CD-ROM und Diskette können gleichzeitig gewählt werden), öffnen Sie durch Rechtsklick das Microsoft Windows-Kontextmenü und wählen Sie den Punkt **Auf Viren untersuchen** (s. Abbildung 27).

Um die Virenuntersuchung einer CD-ROM oder Diskette aus dem Hauptfenster von Kaspersky Anti-Virus zu starten,

1. Legen Sie die CD-ROM oder die Diskette in das entsprechende Laufwerk ein. Beachten Sie, dass das Programm gleichzeitig eine CD-ROM und eine Diskette untersuchen kann.
2. Verwenden Sie den Hyperlink Wechseldatenträger untersuchen auf der linken Seite der Registerkarte **Sicherheit** (s. Abbildung 2). Dieser Hyperlink wird angezeigt, wenn im Infoblock der Aufgabe das Kontrollkästchen **Aufgabe auf Registerkarte "Sicherheit" anzeigen** aktiviert ist (s. Abbildung 28).

   oder

   Wechseln Sie mit Hilfe des Hyperlinks Objekte untersuchen in das Fenster **Untersuchungsobjekte wählen** (s. Abbildung 26), wählen Sie die Wechseldatenträger aus und klicken Sie auf **Untersuchen**.

   oder

   Wählen Sie im Programmhauptfenster die Registerkarte **Einstellungen** und verwenden Sie den Hyperlink Scan auf Befehl. Dadurch wird das Fenster **Scan auf Befehl** (s. Abbildung 28) geöffnet. Wählen Sie in der Liste die Aufgabe **Wechseldatenträger untersuchen** und klicken Sie auf die Schaltfläche **Starten**.

Sofort nach dem Start der Untersuchung erscheint auf dem Bildschirm das Fenster **Untersuchung** (s. Abb. 8). Dieses Fenster informiert über die Ausführung von Aktionen mit den ausgewählten Listenobjekten.

Wenn Sie nur ein Wechselmedium (Gerät) zur Untersuchung gewählt haben, bietet Ihnen Kaspersky Anti-Virus nach dem Abschluss der Untersuchung an, den nächsten Datenträger (Gerät) einzulegen.

Beachten Sie folgende Besonderheiten der Programmfunktion:

- Sollten Sie vergessen haben, vor dem Start der Untersuchung eine CD oder Diskette einzulegen, oder der Wechselspeicher, das Disketten- oder CD-ROM-Laufwerk ist deaktiviert, dann erfolgt keine Untersuchung und das Programm zeigt keinerlei zusätzlichen Meldungen darüber an.
- Wenn Sie die Diskette erst nach dem Start der Untersuchung einlegen, wird er nicht untersucht. Dasselbe gilt für CD-ROMs und andere Wechseldatenträger.
- Wenn Sie während der Untersuchung eine Diskette aus dem Laufwerk entfernt oder ein auswechselbares Laufwerk deaktiviert haben, dann protokolliert das Programm den Fehler, zeigt aber auf dem Bildschirm keinerlei zusätzliche Meldung darüber an. Das Programm fährt mit der Untersuchung des folgenden auswechselbaren Datenträgers fort, falls ein solcher vorhanden ist.

Im Moment der Integration eines Wechseldatenträgers in das System (wenn ein Laufwerk vom Betriebssystem als neues Gerät erkannt wird) untersucht Kaspersky Anti-Virus ein solches Laufwerk auch auf Bootviren, wenn der Echtzeitschutz für Dateien aktiviert ist.

5.4. Bearbeitung von gefundenen schädlichen Objekten

Die Reihenfolge der Aktionen, die Kaspersky Anti-Virus beim Fund eines gefährlichen Objekts, schädlichen Programms oder Objekts, das möglicherweise von einem Virus oder einer Virusmodifikation infiziert ist, hängt vollständig davon ab, welche Einstellungen für den Echtzeitschutz und den Scan auf Befehl festgelegt wurden. In diesem Kapitel wird beschrieben, in welchen Fällen Kaspersky Anti-Virus während der Untersuchung oder bei Untersuchungsende die Auswahl einer Aktion für das gefährliche Objekt anbietet.

Solche Situationen können eintreten, wenn als Aktion für das Objekt gewählt wurde:

- in den Echtzeitschutz-Einstellungen (s. Pkt. 5.2.1.2 auf S. 62) **Benutzer nach Aktion fragen**. In diesem Fall erfolgt die Anfrage nach der Aktion sofort wenn ein gefährliches Objekt gefunden wird.
- in den Einstellungen für Scan auf Befehl (s. Pkt. 5.3.3.2 auf S. 88):

- **Aktion während Untersuchung erfragen**. Die Auswahl einer Aktion für das gefährliche Objekt wird in dem Moment angeboten, wenn Kaspersky Anti-Virus das Objekt findet.

oder

- **Aktion nach Untersuchungsende erfragen**. Die Auswahl der Aktion für gefährliche Objekte erfolgt nur dann, wenn Sie die Bearbeitung dieser Objekte initiiert haben, d.h. durch Klick auf die Schaltfläche **Desinfizieren** im Fenster mit den Untersuchungsergebnissen (s. Abbildung 34).

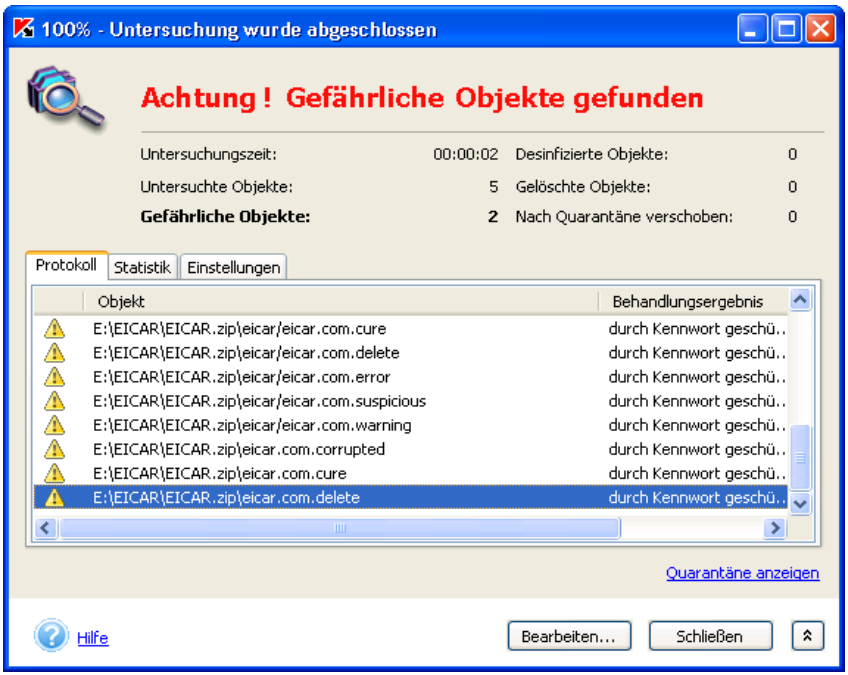

Abbildung 34. Aufgeschobene Bearbeitung von gefährlichen Objekten

Beim Fund eines gefährlichen Objekts erscheint auf dem Bildschirm eine Meldung (s. Abbildung 35) mit folgendem Inhalt:

- ausführliche Beschreibung des Objekts mit dem Namen des gefährlichen Programms.
- Auswahl von Aktionen, die Sie mit dem Objekt ausführen können. Eine der angebotenen Aktionen wird jeweils von Kaspersky-Lab-Experten zur Behandlung des Objekts empfohlen. Neben dieser Aktion steht

(empfohlen). Außerdem können Ihnen folgende Aktionen zur Auswahl angeboten werden (Die Liste der angebotenen Aktionen hängt von der Art des gefundenen Objekts ab):

- **Desinfizieren** – Es wird versucht, das infizierte Objekt zu desinfizieren, wenn dessen Desinfektion möglich ist. Bei der erstmaligen Desinfektion eines Objekts wird eine Kopie im Backup-Speicher angelegt.
- **Löschen** – Das infizierte oder möglicherweise infizierte Objekt wird gelöscht. Beim Löschen eines Objekts wird eine Kopie im Backup-Speicher angelegt.
- **Überspringen** – Es werden keine Aktionen mit dem Objekt ausgeführt, sondern nur Informationen darüber protokolliert.

Das gefährliche Objekt wird übersprungen, wenn Sie die Meldung über den Fund mit Hilfe der Schaltfläche in der rechten oberen Ecke schließen.

- **Nach Quarantäne verschieben** – Das Objekt, das möglicherweise von einem Virus oder einer Virusmodifikation infiziert ist, wird unter Quarantäne gestellt. Dort kann es später unter Verwendung aktualisierter Antiviren-Datenbanken erneut untersucht, wiederhergestellt, zur Analyse an Kaspersky Lab geschickt oder gelöscht werden.
- **Überspringen, zu Ausnahmen hinzufügen** – Das gefundene Programm zur Liste der Ausnahmen für die Antivirenuntersuchung und den Echtzeitschutz hinzufügen.

Damit eine hinzugefügte Ausnahme verwendet wird, ist es notwendig, im Fenster **Liste der Ausnahmen** das Kontrollkästchen **Allgemeine Liste der Ausnahmen verwenden** zu aktivieren (s. Abbildung 38).

Kaspersky Anti-Virus for Windows Workstations
Achtung! Ein virusinfiziertes Objekt wurde gefunden.
Objekt C:\...\eicar\eicar.com.cure ist infiziert von Virus EICAR-Test-File. Wir empfehlen die Desinfektion dieses Objekts.
Desinfizieren (empfohlen)
Löschen
Überspringen
Anwenden auf alle infizierten Objekte, deren Desinfektion möglich ist (während dieser Sitzung)
Hilfe
Tonsignale AUS
OK

Abbildung 35. Meldung beim Fund eines infizierten Objekts

Sie können die gewählte Aktion außerdem auf alle Objekte des gleichen Typs anwenden, indem Sie das entsprechende Kontrollkästchen aktivieren. Um die Aktion beispielsweise auf alle infizierten Objekte anzuwenden, die vom Programm desinfiziert werden können, aktivieren Sie das Kontrollkästchen ☑ **Anwenden auf alle infizierten Objekte, deren Desinfektion möglich ist (während dieser Sitzung)**.

Wenn Sie die Behandlung von Objekten aus irgendeinem Grund abgelehnt und die Variante **Überspringen** gewählt haben, können Sie später zur Bearbeitung zurückkehren. Verwenden Sie dazu auf der rechten Seite der Registerkarte **Sicherheit** den Hyperlink diese Objekte zu bearbeiten. Dadurch wird das Dialogfenster **Gefundene gefährliche Objekte** (s. Abbildung 36) geöffnet, das eine ausführliche Beschreibung jedes gefährlichen Objekts sowie einen Link zu der entsprechenden Beschreibung in der Viren-Enzyklopädie auf der Seite www.viruslist.com/de enthält.

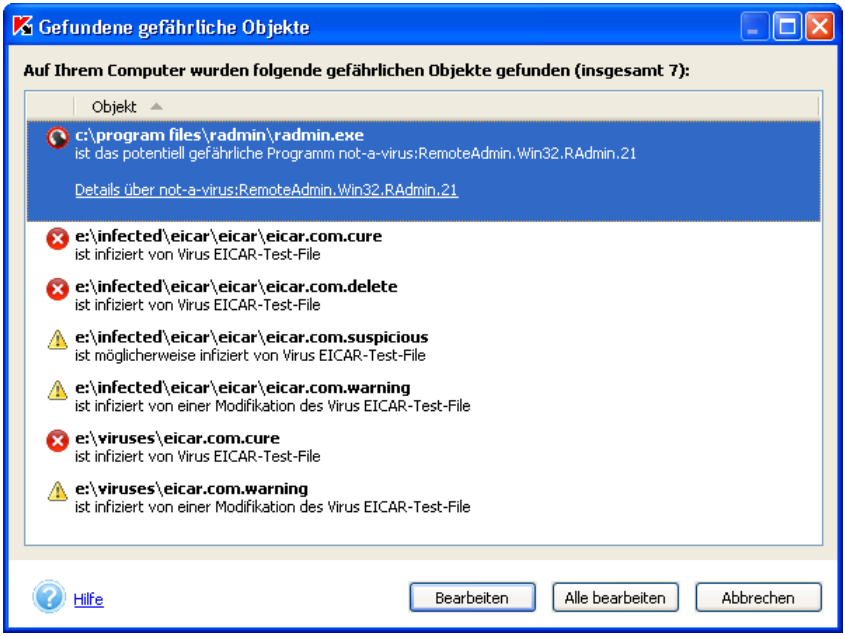

Abbildung 36. Liste der gefundenen gefährlichen Objekte

Mit Hilfe der Schaltfläche **Bearbeiten** können Sie ein aus der Liste ausgewähltes Objekt bearbeiten. Mit Hilfe der Schaltfläche **Alle bearbeiten** können Sie die Bearbeitung aller Objekte der Liste starten. Während er Bearbeitung werden Meldungen auf dem Bildschirm angezeigt (s. Abbildung 35), in denen Sie eine Aktion für das Objekt wählen können (detaillierte Beschreibung der möglichen Aktionen siehe oben).

Um ein unbearbeitetes Objekt aus der Liste zu löschen, verwenden Sie den Kontextmenübefehl **Aus der Liste löschen** (s. Abb. 37).

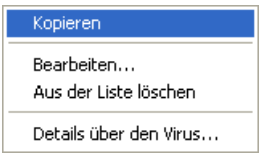

Abbildung 37. Kontextmenü des Fensters **Gefundene gefährliche Objekte**

Wenn eines der gefährlichen Objekte manuell gelöscht worden ist, dann erscheint es beim Bearbeitungsversuch nicht mehr in der Liste der gefundenen gefährlichen Objekte.

5.5. Aktivitätskontrolle der Programmprozesse

In Kaspersky Anti-Virus besteht die Möglichkeit, eine Liste der Programmprozesse anzulegen, deren Dateiaktivität von der Antivirenanwendung nicht kontrolliert werden soll.

Wenn Sie beispielsweise die Objekte, die von dem standardmäßigen Microsoft Windows-Programm **Editor** verwendet werden, für ungefährlich und deren Untersuchung im Echtzeitschutz nicht für erforderlich halten, bedeutet das, dass Sie dem Prozess dieses Programms vertrauen. Um die Objekte, die von diesem Prozess benutzt werden, von der Untersuchung auszuschließen, fügen Sie das Programm **Editor** zur Liste der vertrauenswürdigen Prozesse hinzu.

Um die Liste der vertrauenswürdigen Prozesse zu bearbeiten,

verwenden Sie auf der Registerkarte **Dateien** (s. Abbildung 16) im Abschnitt **Schutz-Einstellungen** den Hyperlink nicht festgelegt/ festgelegt neben dem Parameter **Vertrauenswürdige Prozesse**.

Dadurch wird das Fenster **Liste der Ausnahmen** (s. Abbildung 38) geöffnet. Ergänzen oder ändern Sie die Liste mit Hilfe der rechts angebrachten Schaltflächen.

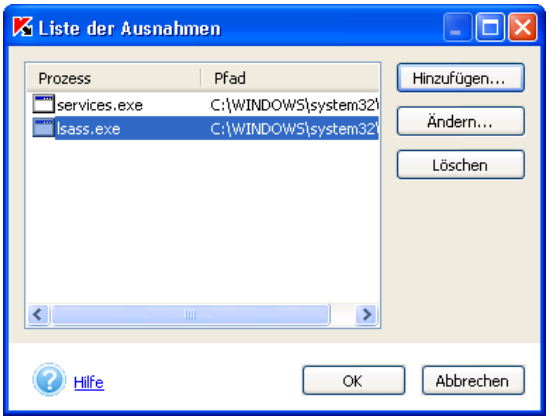

Abbildung 38. Fenster zum Anpassen der Liste mit vertrauenswürdigen Prozessen

Mit Hilfe der Schaltfläche **Hinzufügen** können Sie Ausnahmen zur Liste hinzufügen:

- *ausführbare Datei*. Verwenden Sie dazu den Befehl **Durchsuchen** und geben Sie eine Datei mit der Erweiterung **.exe** an.
- *gestarteter Prozess*. Verwenden Sie dazu den Befehl **Gestartete Prozesse** und wählen Sie in der Dropdown-Liste einen aktiven Prozess aus.

Um einen Prozess aus der Liste zu entfernen, wählen Sie den betreffenden Prozess und klicken Sie auf **Löschen**.

Durch Klick auf die Schaltfläche **Ändern** wird ein zusätzliches Fenster geöffnet (s. Abbildung 39).

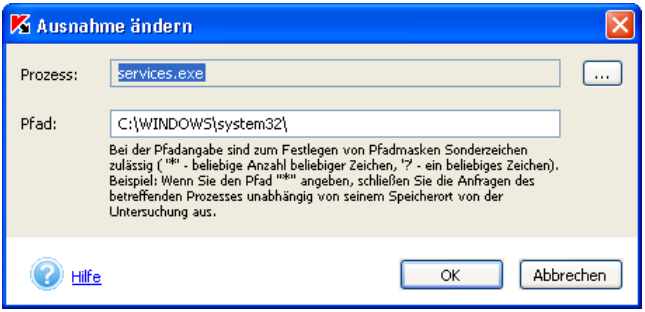
Ausnahme ändern
Prozess:
services.exe
...
Pfad:
C:\WINDOWS\system32\
Bei der Pfadangabe sind zum Festlegen von Pfadmasken Sonderzeichen zulässig ('*' - beliebige Anzahl beliebiger Zeichen, '?' - ein beliebiges Zeichen). Beispiel: Wenn Sie den Pfad "*" angeben, schließen Sie die Anfragen des betreffenden Prozesses unabhängig von seinem Speicherort von der Untersuchung aus.
Hilfe
OK
Abbrechen

Abbildung 39. Hinzufügen eines vertrauenswürdigen Prozesses

Der Dateiname des Prozesses kann mit Hilfe der Schaltfläche . Bei der Auswahl eines Namens speichert Kaspersky Internet Security die internen Attribute der Prozessdatei, mit denen der Prozess bei der Untersuchung als vertrauenswürdig identifiziert wird.

Der Pfad der Datei wird bei der Auswahl des Namens automatisch ergänzt. Der Pfad kann manuell geändert werden.

Geben Sie als Pfad den vollständigen Pfad der Prozessdatei oder die Maske * (beliebige Anzahl von beliebigen Zeichen) oder **?** (ein beliebiges Zeichen) an.
Bei der Verwendung der Maske * wird ein gestarteter Prozess beispielsweise unabhängig vom Speicherort der Prozessdatei als vertrauenswürdig eingestuft.

Aktivieren Sie im Fenster **Liste der Ausnahmen** (s. Abbildung 38) das Kontrollkästchen **Zugelassene potentiell gefährliche Software ausschließen**, wenn Sie möchten, dass die zugelassenen Programme von der Untersuchung ausgeschlossen werden. Diese Programme werden im Fenster **Bedrohungen und Ausnahmen** genannt, das mit der Schaltfläche **Details** geöffnet wird (s. Pkt. 5.7 auf S. 102).

5.6. Benutzeraufgaben

Bei Installation von Kaspersky Anti-Virus wird ein Satz von Systemaufgaben angelegt. Diese enthält die Aktualisierungsaufgaben (Update der Antiviren-Datenbanken, Update von Programmmodulen, Rückgängigmachen des Updates der Antiviren-Datenbank) und Untersuchungsaufgaben (Vollständige Untersuchung von Mein Computer, Automatische Untersuchung beim Start von Kaspersky Anti-Virus, Untersuchung von Wechseldatenträgern, Untersuchung der Quarantäne).

Sie können die Systemaufgaben aufrufen, deren Optionen und Zeitplan anpassen. Die Daten in den Aufgaben können nicht gelöscht werden.

Die Einstellung der Optionen für die Aufgabe Update der Datenbanken und Komponenten wurde in Kapitel 5 auf S. 43 beschrieben. Die Aufgabe Rückgängigmachen der zuletzt ausgeführten Updates hat keine spezifischen Einstellungen.

Bei der Arbeit mit Kaspersky Anti-Virus kann der Administrator Untersuchungsaufgaben für Benutzerobjekte anlegen und deren Funktionen verwalten.

Ein Benutzer der Workstation kann Aufgaben nicht anlegen und einstellen. Er kann die Liste mit Aufgaben, die vom Administrator angelegt wurde, im linken Teil der Registerkarte **Sicherheit** (s. Abbildung 2) anzeigen und sie ausführen lassen.

Wenn Sie für Kaspersky Anti-Virus entfernt steuern, werden der Aufgabenliste lokale Aufgaben und Gruppenaufgaben hinzugefügt, die über Kaspersky Administration Kit erstellt werden (s. Pkt. 6.3 auf S. 172). Die Steuerung lokaler Aufgaben entspricht der Steuerung von Aufgaben, die vom Benutzer erstellt wurden: sie können gestartet, gelöscht und angepasst werden. Gruppenaufgaben können nicht gestartet, gelöscht oder angepasst werden, da die Steuerung dieser Aufgaben nur über die Anwendung Kaspersky Administration Kit erfolgt.

Wenn bei der Steuerung von Aufgaben über die Anwendung Kaspersky Administration Kit das Verändern bestimmter Parameter verboten wurde (das "Schloss" wurde geschlossen), dann können sie nicht über die lokale Oberfläche von Kaspersky Anti-Virus angepasst werden.

Um eine neue Aufgabe zu erstellen,

verwenden Sie die Schaltfläche **Neu** im Fenster **Scan auf Befehl** (s. Abbildung 28). Daraufhin wird ein Fenster (s. Abbildung 29) geöffnet, das folgende Registerkarten enthält: **Untersuchungsobjekte**, **Einstellungen**, **Zeitplan** und **Rechte für den Start**.

Geben Sie im Feld **Aufgabenname** den Namen der Aufgabe an und nehmen Sie die übrigen Einstellungen vor (Details s. Pkt. 5.3.3 auf S. 82).

Die Einstellungen jeder Aufgabe enthalten das Kontrollkästchen **Aufgabe auf der Registerkarte "Sicherheit" anzeigen** das die Anzeige der Aufgabe im Programmhauptfenster reguliert. Wenn das Kontrollkästchen aktiviert ist, ist die Aufgabe für den Benutzer der Workstation auf der linken Seite der Registerkarte sichtbar und kann zur Ausführung gestartet werden.

Um eine Aufgabe aus der Liste zu löschen, wählen Sie sie aus und klicken Sie auf **Löschen**. Beachten Sie, dass nur jene Aufgaben aus der Liste entfernt werden können, die manuell hinzugefügt wurden. Systemaufgaben sowie Gruppenaufgaben, die über Kaspersky Aministration Kit erstellt wurden, können nicht entfernt werden.

Um eine Aufgabe zur Ausführung zu starten, wählen Sie sie in der Liste aus und klicken Sie auf **Starten**. Dabei erscheint ein Fenster, das über den Verlauf der Aufgabenausführung informiert.

Zur Anzeige der Parameter einer erstellten Aufgabe, wählen Sie sie in der Liste aus und klicken Sie auf **Eigenschaften**.

5.7. Erstellen einer Ausnahmenliste

In bestimmten Situationen kann es erforderlich sein, bestimmte Objekte von der Untersuchung oder vom Schutz auszuschließen. Sie können eine Liste von Ausnahmen erstellen, die für Scan auf Befehl, Datei-Echtzeitschutz und E-Mail-Echtzeitschutz gelten.

Die gemeinsame Liste aller Ausnahmen für den Antivirenschutz des Computers kann in dem dafür vorgesehenen Fenster **Bedrohungen und Ausnahmen** überprüft und geändert werden (s. Abbildung 14). Verwenden Sie den Hyperlink Bedrohungen und Ausnahmen auf der linken Seite der Registerkarte **Einstellungen** (s. Abb. 6), um das Fenster zu öffnen. Die Liste der Ausnahmen wird mit Hilfe der entsprechenden Schaltflächen bearbeitet.

*Um eine Ausnahme hinzuzufügen, klicken Sie auf **Hinzufügen**.*

Dadurch wird das Fenster **Auszuschließendes Objekt** (s. Abbildung 40) geöffnet, in dem Sie die Ausnahme für Kaspersky Anti-Virus festlegen können.

Als Ausnahmen können festgelegt werden:

- *Laufwerke, Ordner, Dateien, Dateimasken*.

- *Bedrohungen* – Typen *schädlicher* oder potentiell gefährlicher Programme.
- *Dateien bestimmter Bedrohungstypen* – konkrete Dateien, denen nach der Untersuchung bestimmte Bedrohungstypen zugewiesen werden.

Um einen bestimmten Ordner oder Dateien (nach Maske) vom Schutz durch Kaspersky Anti-Virus auszuschließen,

füllen Sie das Feld **Objekt** mit Hilfe der Schaltfläche ... aus.

Abbildung 40. Liste der Ausnahmen erstellen

Bei der Angabe des Pfads für einen Ordner oder ein Objekte können Sie Systemumgebungsvariable verwenden. Für die Untersuchung des Installationsordners des Betriebssystems Microsoft Windows können Sie beispielsweise die Variable **%windir%** verwenden.

Es können gleichzeitig mehrere, durch "Leerzeichen" getrennte Masken hinzugefügt werden. Wenn ein Dateiname ein "Leerzeichen" enthält, muss der Name in Anführungszeichen gesetzt werden.

Es folgen Beispiele für zulässige Ausschlussmasken:

- Masken ohne Pfade der Objekte:

  ***.exe** – alle Dateien mit der Erweiterung *exe*

  ***.ex?** – alle Dateien mit der Erweiterung *ex?*, wobei anstelle von ? ein beliebiges Zeichen stehen kann.

  test – alle Dateien mit dem Namen *test*

- Masken mit absoluten Pfaden der Objekte:

  C:\dir*.* – alle Dateien im Ordner *C:\dir*

  C:\dir*.exe – alle Dateien mit der Erweiterung *exe* im Ordner *C:\dir*

C:\dir*.ex? – alle Dateien mit der Erweiterung *ex?* im Ordner *C:\dir*, wobei anstelle von ? ein beliebiges Zeichen stehen kann.

C:\dir\test – nur die Datei *C:\dir\test*

C:\dir – alle Dateien im Ordner *C:\dir* und allen seinen Unterordnern

- Masken mit relativen Pfaden der Objekte:

  dir*.* – alle Dateien in allen Ordnern von *dir*

  dir\test – alle Dateien *test* in den Ordnern von *dir*

  dir*.exe – alle Dateien mit der Erweiterung *exe* in allen Ordnern von *dir*

  dir*.ex? – alle Dateien mit der Erweiterung *ex?* in allen Ordnern von *dir*, wobei anstelle von ? ein beliebiges Zeichen stehen kann.

  dir – alle Dateien in allen Ordnern von *dir* und allen seinen Unterordnern

Es wird davor gewarnt, die Maske *.* oder * als Ausnahme anzugeben, weil das dem Deaktivieren des Echtzeitschutzes gleichkommt.

Es wird davor gewarnt, als Ausnahme ein virtuelles Laufwerk auszuwählen, das auf der Basis eines Ordners des Dateisystems mit Hilfe des Befehls *subst* erstellt wurde. Dies wäre sinnlos, da Kaspersky Anti-Virus während der Untersuchung dieses virtuelle Laufwerk als Ordner betrachtet und folglich untersucht.

Um alle Dateien von der Antiviren-Bearbeitung auszuschließen, denen aufgrund der Untersuchung ein bestimmter Bedrohungstyp zugewiesen wurde,

blenden Sie mit Hilfe der Schaltfläche den erweiterten Teil des Fensters (s. Abbildung 40) ein und wählen Sie die Bedrohung im Fenster **Liste der erkennbaren Bedrohungen** (s. Abbildung 41), das mit Hilfe der Schaltfläche geöffnet wird.

In diesem Fenster können Sie eine Bedrohung nach ihrem Namen suchen, die Liste der Bedrohungen durch Klick auf die Überschrift der Spalte **Name** sortieren und den Namen einer Bedrohung in die Zwischenablage kopieren (mit Hilfe des entsprechenden Kontextmenübefehls). Außerdem können Sie auf der Seite www.viruslist.com eine ausführliche Beschreibung der Bedrohung lesen.

Wählen Sie dazu die Bedrohung in der Liste aus und verwenden Sie den Befehl **Details** im Kontextmenü.

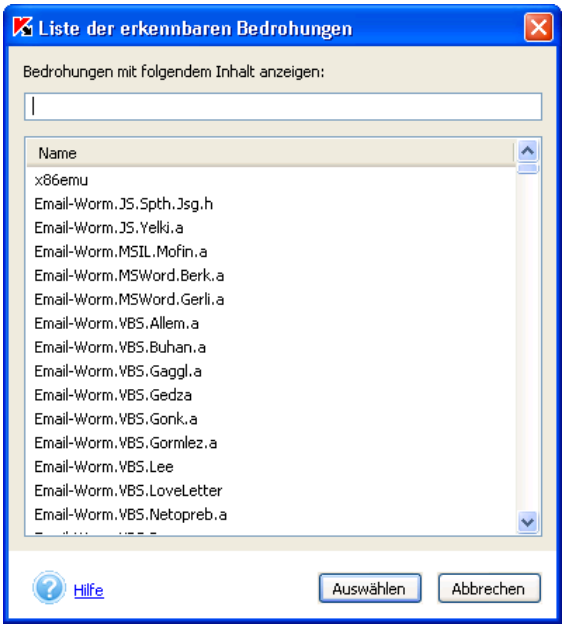

Abbildung 41. Liste der erkennbaren Bedrohungen

Um ein konkretes Objekt mit einem Ihnen bekannten Bedrohungstyp vom Schutz auszuschließen,

1. Geben Sie im Feld **Objekt** den Namen des Objekts an.
2. Geben Sie im Feld **Bedrohung** den Typ der Bedrohung an.

Eine Datei mit einem bestimmten Bedrohungstyp kann auch vom Meldungsfenster aus ausgeschlossen werden, das beim Fund einer solchen Datei von Kaspersky Anti-Virus geöffnet wird (s. Abbildung 42). Wenn Sie der Meinung sind, dass dieses Programm ungefährlich ist und auf Ihrem Computer verwendet werden kann, wählen Sie die Variante **Zur Liste der erlaubten Programme hinzufügen**. Das Programm wird zur Liste der Untersuchungsausnahmen im Fenster **Bedrohungen und Ausnahmen** (s. Abbildung 14) hinzugefügt.

Kaspersky Anti-Virus for Windows Workstations
Achtung! Ein potentiell gefährliches Programm wurde gefunden.
Der Zugriff auf Objekt C:\...\Desktop\1.ex wurde gesperrt. Objekt ist das potentiell gefährliche Programm not-a-virus:Downloader.Win3....
Überspringen
Löschen
Überspringen, zu Ausnahmen hinzufügen
Anwenden auf alle infizierten Objekte, deren Desinfektion nicht möglich ist (während dieser Sitzung)
Potentiell gefährliche Software: ein Programm oder Elemente eines Programms, die ein Angreifer benutzen kann, um illegale Aktionen mit Informationsressourcen des Computers oder lokalen Netzwerks auszuführen.
Wird die Verwendung des Programms vom Benutzer erlaubt, dann muss es den Ausnahmen hinzugefügt und somit von der Untersuchung ausgeschlossen werden.
Hilfe
Tonsignale AUS
OK

Abbildung 42. Meldung über eine Bedrohung

5.8. Konfiguration des Zeitplans

Für die Aufgaben zum Scan auf Befehl und zum Update kann ein Zeitplan für den automatischen Start erstellt werden. Das erlaubt Ihnen den rechtzeitigen Download der Updates für die Antiviren-Datenbanken und die regelmäßige Untersuchung der Objekte Ihres Computers mit den aktuellen Datenbanken.

Kaspersky Anti-Virus aktualisiert die Antiviren-Datenbanken standardmäßig alle drei Stunden und führt jeden Freitag um 20:00 Uhr die vollständige Untersuchung des Computers durch.

Um den Zeitplan für das Update der Antiviren-Datenbanken zu ändern,

1. Verwenden Sie den Hyperlink Update, der sich auf der linken Seite der Registerkarte **Einstellungen** befindet.
2. Wählen Sie im folgenden Fenster die Aufgabe, für welche der Zeitplan erstellt bzw. angepasst werden soll, und klicken Sie auf die Schaltfläche **Eigenschaften**.

Dadurch wird das Fenster mit den Update-Einstellungen auf der Registerkarte **Zeitplan** geöffnet (s. Abbildung 8).

Um einen Zeitplan für die Aufgaben zum Scan auf Befehl zu erstellen/ändern,

1. Verwenden Sie den Hyperlink Scan auf Befehl, der sich auf der linken Seite der Registerkarte **Einstellungen** befindet.
2. Wählen Sie im Fenster mit der Liste der Untersuchungsaufgaben (s. Abbildung 28) die Aufgabe aus, für welche Sie einen Zeitplan erstellen/ändern möchten, und klicken Sie auf die Schaltfläche **Eigenschaften**.

Dadurch wird ein Fenster zur detaillierten Einstellung dieser Aufgabe geöffnet (s. Abbildung 29). Der Zeitplan wird auf der Registerkarte **Zeitplan** angepasst (s. Abbildung 43).

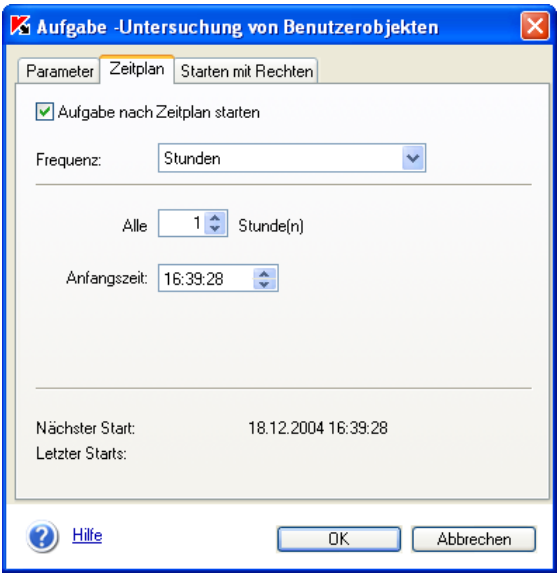

Abbildung 43. Erstellen einer neuen Aufgabe. Registerkarte **Zeitplan**

Um den automatischen Aufgabenstart nach Zeitplan anzuschalten, aktivieren Sie das Kontrollkästchen **Zeitgesteuerten Aufgabenstart aktivieren**.

Wenn Sie über das bevorstehende Update benachrichtigt werden möchten, aktivieren Sie das Kontrollkästchen **Vor dem Start der geplanten Aufgabe nach Bestätigung fragen**. Wenn dieses Kontrollkästchen aktiviert ist, wird auf dem Bildschirm das Fenster **Aufgabenstart nach Zeitplan** (s. Abbildung 44)

angezeigt, bevor der Start nach Zeitplan gestartet wird. Klicken Sie auf die Schaltfläche **Starten**, um die zeitgesteuerten Untersuchung zu starten. Wenn Sie die Untersuchung für einen bestimmten Zeitraum zurückstellen möchten, wählen Sie das gewünschte Intervall in der Dropdown-Liste und klicken Sie auf **Aufschieben**. Wenn der Benutzer im Dialogfenster innerhalb von 3 Minuten keine Aktion wählt, wird die Aufgabe automatisch gestartet.

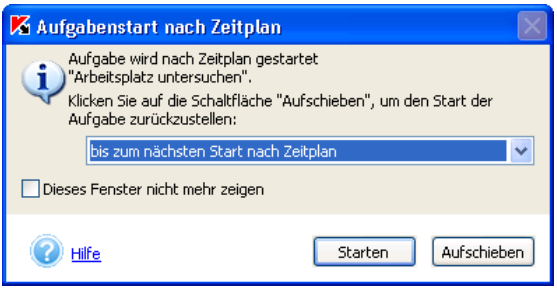
Aufgabenstart nach Zeitplan
Aufgabe wird nach Zeitplan gestartet "Arbeitsplatz untersuchen".
Klicken Sie auf die Schaltfläche "Aufschieben", um den Start der Aufgabe zurückzustellen:
bis zum nächsten Start nach Zeitplan
Dieses Fenster nicht mehr zeigen
Hilfe
Starten
Aufschieben

Abbildung 44. Anfrage zum Aufgabenstart nach Zeitplan

Wählen Sie im Feld **Frequenz** einen Wert für das Intervall, in dem die Aufgabe ausgeführt werden soll. Folgende Varianten sind möglich: *Stunden, Tage, Wochen, bei Programmstart*. Abhängig von der gewählten Variante verändert der mittlere Teil des Fensters mit den Feldern zur Dateneingabe sein Aussehen:

- *Stunden*: Die Aufgabe wird nach Zeitplan im Abstand einer bestimmten Anzahl von Stunden zur Ausführung gestartet. Legen Sie das Intervall (in Stunden) und die Uhrzeit des ersten Starts fest.

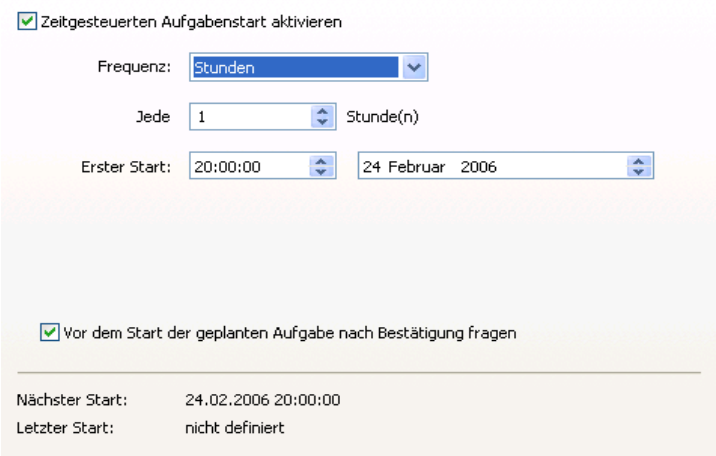

Abbildung 45. Anpassen des Zeitplans nach Stunden

- *Tage*: Die Aufgabe wird nach Zeitplan im Abstand einer bestimmten Anzahl von Tagen zur Ausführung gestartet. Legen Sie das Intervall (in Tagen) und die Uhrzeit des Starts fest.

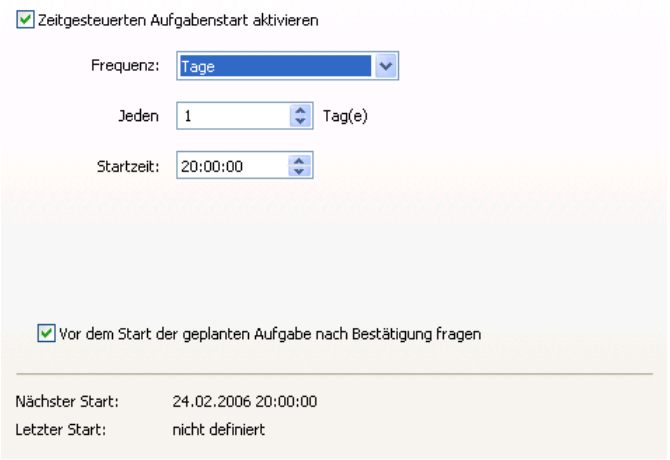

Abbildung 46. Anpassen des Zeitplans nach Tagen

- *Wochen*: Die Aufgabe wird nach Zeitplan im Abstand einer bestimmten Anzahl von Wochen zur Ausführung gestartet. Legen Sie das Intervall (in Wochen), den Wochentag und die Startuhrzeit fest.

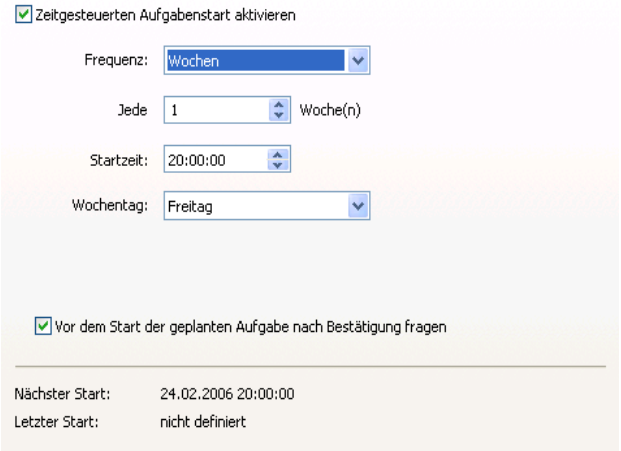

Abbildung 47. Anpassen des Zeitplans nach Wochen

- *Bei Programmstart*: Die Aufgabe wird sofort nach dem Start von Kaspersky Anti-Virus zur Ausführung gestartet.

5.9. Aufgabenstart im Namen eines bestimmten Benutzers

In Kaspersky Anti-Virus wurde ein Dienst zum Starten von Benutzeraufgaben unter dem Namen eines anderen Benutzerkontos realisiert.

Dieser Dienst ist standardmäßig deaktiviert und die Aufgaben werden unter dem Namen des aktiven Benutzerkontos gestartet. Bei Verwendung des Diensts gibt der Administrator die Daten des Benutzerkontos ein, das über ausreichende Rechte für den Zugriff auf ein Objekt verfügt: Zum Beispiel sind zur Ausführung von Aufgaben für den Scan auf Befehl die Zugriffsrechte für das zu untersuchende Objekt erforderlich, und zur Ausführung von Updateaufgaben die Zugriffsrechte für den lokalen Updateordner oder die Rechte eines autorisierten Proxyserverbenutzers.

Dadurch können bei der Ausführung von Aufgaben zum Scan auf Befehl und von Updateaufgaben Fehler vermieden werden, wenn der Benutzer, der die Aufgabe startet, nicht über die erforderlichen Zugriffsrechte verfügt.

Die Konfiguration des Starts von Antiviren-Aufgaben unter dem Namen eines anderen Benutzerkontos erfolgt auf der Registerkarte **Rechte für den Start** (s. Abbildung 48).

Um diesen Dienst zu anzuschalten, aktivieren Sie das Kontrollkästchen **Aufgabe starten im Namen des Benutzers**. Dieses Kontrollkästchen ist standardmäßig deaktiviert und der Aufgabenstart erfolgt mit den Rechten des aktiven Benutzerkontos.

Geben Sie unten die Daten des Benutzerkontos ein, unter dem die Aufgabe gestartet wird: Benutzername und Kennwort.

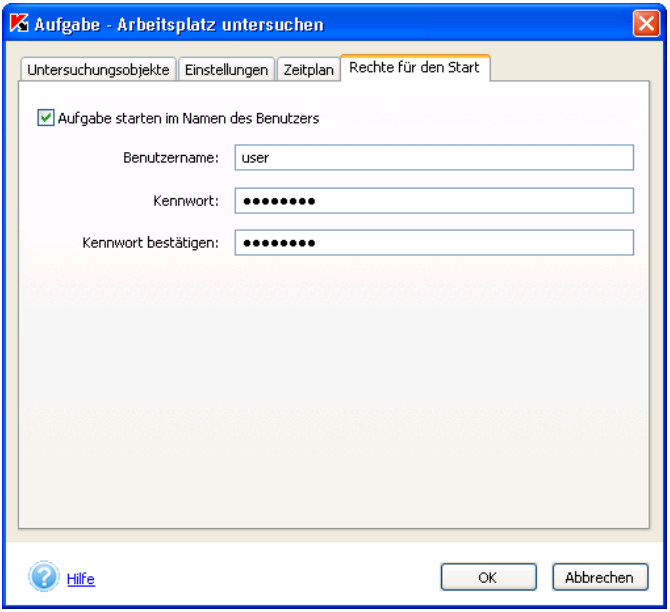

Abbildung 48. Registerkarte **Rechte für den Start**

5.10. Zusatzeinstellungen

Kaspersky Anti-Virus bietet Ihnen folgende Möglichkeiten zum Anpassen und zur Arbeit mit dem Produkt:

- Arbeit mit verdächtigen Objekten, die in die Quarantäne verschoben wurden.
- Arbeit mit den Kopien von Objekten, die bei der Arbeit von Kaspersky Anti-Virus gelöscht oder verändert und im Backup-Speicher gespeichert wurden.
- Anzeige des Protokolls über die Arbeit des Programms.
- Verwaltung der Konfiguration von Kaspersky Anti-Virus.
- Erweiterte Einstellungen.
- Einstellungen der Eingabeaufforderungen.
- Arbeit im Administrator- oder Benutzermodus.

5.10.1. Quarantäne und Backup

Kaspersky Anti-Virus stellt eine Funktion zur Isolierung von verdächtigen Objekten in eine Quarantäne und zur Aufbewahrung der Kopien von infizierten Objekten in der Backup-Ablage vor der Reparatur oder Löschung zur Verfügung.

Beim Entdecken eines verdächtigen Objektes isoliert das Programm es in ein Quarantäne-Verzeichnis, wo das Objekt eingehender analysiert, gelöscht, wiederhergestellt oder zur Analyse an Kaspersky Lab eingeschickt werden kann.

Die Sicherheitskopie wird beim ersten Ausführen einer Reparatur oder beim Löschen des Objektes nach dem Entdecken angelegt und im Backup aufbewahrt, wo das Objekt wiederhergestellt werden kann, wenn es einen informativen Wert hat.

5.10.1.1. Einstellungen der Optionen für Quarantäne und Backup

Um die Einstellungen für die Quarantäne und den Backup-Speicher anzuzeigen oder zu ändern,

klicken Sie auf den Hyperlink Quarantäne und Backup auf der linken Seite der Registerkarte **Einstellungen**.

Auf den Registerkarten des Fensters **Quarantäne- und Backup-Einstellungen** können Sie die Optionen einstellen.

Nehmen Sie im folgenden Fenster (s. Abbildung 49) auf den entsprechenden Registerkarten die gewünschten Änderungen für Quarantäne und Backup vor:

- **Gespeicherte Objekte löschen nach ... (Tagen)**. Die Speicherdauer für Dateien in Quarantäne ist standardmäßig unbegrenzt (das Kontrollkästchen ist deaktiviert). Sie können die Speicherdauer für Dateien begrenzen, indem Sie das Kontrollkästchen aktivieren und im Eingabefeld die gewünschte Anzahl von Tagen festlegen (als Standard gelten 90 Tage).
- **Maximale Größe (MB)**. Die Größe der Quarantäne ist standardmäßig nicht beschränkt (das Kontrollkästchen ist deaktiviert). Sie können die Gesamtgröße der im Quarantäneordner gespeicherten Dateien begrenzen, indem Sie dieses Kontrollkästchen aktivieren und im Eingabefeld die gewünschte Größe festlegen (als Standard gelten 100 MB). Wählen Sie darunter die Aktion, die von Kaspersky Anti-Virus ausgeführt werden soll, wenn die maximale Größe des Speichers überschritten wird:

- *Benutzer informieren* – Beim Erreichen der maximalen Größe erscheint auf dem Bildschirm eine Meldung mit einer Anfrage nach dem weiteren Vorgehen.
- *Alte Objekte löschen* – Dateien löschen, die am sich am längsten unter Quarantäne befinden.

Quarantäne-Objekte nach jedem Update der Antiviren-Datenbanken automatisch untersuchen. Dieser Modus von Kaspersky Anti-Virus erlaubt es, die Quarantäneobjekte nach jedem Datenbank-Update automatisch zu untersuchen.

Kaspersky Anti-Virus kann die Quarantäneobjekte nicht sofort nach dem Update der Antiviren-Datenbanken untersuchen, wenn Sie in diesem Moment mit der Quarantäne arbeiten.

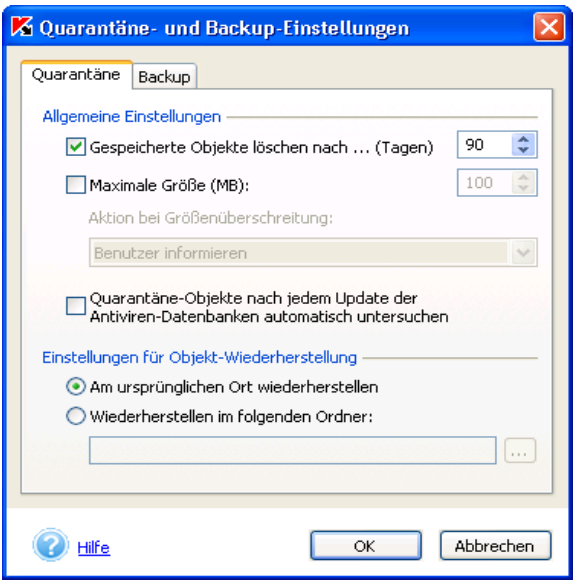

Abbildung 49. Einstellung der Quarantäne-Optionen

Legen Sie im Abschnitt **Einstellungen für Objekt-Wiederherstellung** fest, wohin Objekte bei der Wiederherstellung aus dem Speicher verschoben werden sollen:

Am ursprünglichen Ort wiederherstellen. Standardmäßig wird die wiederhergestellte Kopie dort gespeichert, wo Kaspersky Anti-Virus das Originalobjekt gefunden hat.

Wiederherstellen im folgenden Ordner. Geben Sie bei Auswahl dieser Variante den Pfad des Ordners an, in dem wiederherzustellende Objekte gespeichert werden sollen.

Die Einstellungen für die maximale Größe des Backup-Speichers, die Speicherdauer und die Wiederherstellung von Sicherungskopien entsprechen den Quarantäne-Einstellungen.

5.10.1.2. Arbeit mit der Quarantäne

Alle verdächtigen Objekte, die bei einer Virensuche im Computer erkannt oder im Echtzeitschutz abgefangen werden, werden von Kaspersky Anti-Virus in die Quarantäne verschoben, wo Sie die Arbeit mit diesen Objekten (untersuchen, wieder herstellen, löschen usw.) fortsetzen können.

Standardmäßig untersucht Kaspersky Anti-Virus nach jedem Update der Antiviren-Datenbanken die in der Quarantäne befindlichen Objekte. Falls Sie die Quarantäne-Objekte manuell untersuchen müssen, empfehlen wir Ihnen, die Antiviren-Datenbanken upzudaten. Möglicherweise enthalten in diesem Moment die Datenbanken bereits einen Eintrag über verdächtige Viren, die Dateien befallen können und wie sie repariert werden können.

Die Arbeit mit verdächtigen Objekten wird im Fenster **Quarantäne** (s. Abbildung 50) verwaltet, das sich mit einem Klick auf den Hyperlink Quarantäne auf der Registerkarte **Sicherheit** (s. Abbildung 2) des Programmhauptfensters oder auf den Hyperlink Quarantäne im Fenster Vollständige Untersuchung (s. Abbildung 5).

Auf der Registerkarte **Sicherheit** (s. Abbildung 2) wird neben dem Hyperlink Quarantäne in Klammern die Gesamtzahl der Objekte angegeben, die sich in der Quarantäne befinden.

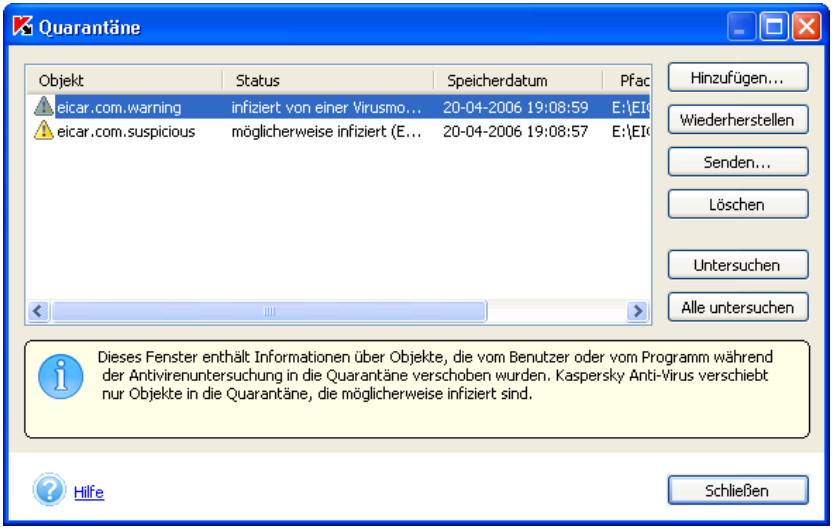

Abbildung 50. Fenster mit Quarantäne-Objekten

In diesem Dialogfenster können Sie folgende Aktionen ausführen:

- Eine Datei, die Sie für verdächtig halten, in der Kaspersky Anti-Virus aber keinen Virus gefunden hat, in die Quarantäne verschieben. Klicken Sie dazu auf **Hinzufügen** und geben Sie im Standardauswahlfenster die möglicherweise infizierte Datei an. Sie wird mit dem Status *Vom Benutzer verschoben* in die Liste aufgenommen.

- Untersuchung und Desinfektion aller möglicherweise infizierten Objekte oder nur der aus der Liste ausgewählten Objekte unter Verwendung der aktuellen Antiviren-Datenbanken. Klicken Sie dazu auf **Alle untersuchen** oder **Untersuchen** (nachdem die zu untersuchenden Objekte ausgewählt wurden).

  Als Ergebnis der Untersuchung und Desinfektion eines Quarantäne-objekts kann sich sein Status in *infiziert*, *möglicherweise infiziert*, *Fehlalarm*, *virusfrei* usw. ändern.

  Der Objektstatus *infiziert* bedeutet, dass das Objekt als gefährlich identifiziert wurde, seine Desinfektion aber erfolglos war. Wir empfehlen Ihnen, Objekte mit diesem Status zu löschen.

  Alle Objekte mit dem Status *Fehlalarm* können gefahrlos wiederhergestellt werden, da ihr vorheriger Status *möglicherweise infiziert* nicht von Kaspersky Anti-Virus bestätigt wurde.

Die Aufgabe **Quarantäne untersuchen** kann im Fenster **Scan auf Befehl** (s. Abbildung 28) gestartet werden. Beim Start der Aufgabe wird auf dem Bildschirm das Fenster **Untersuchung wird ausgeführt** (s. Abbildung 5) geöffnet. Die Untersuchungsergebnisse können in einem Protokoll überprüft werden (Details s. Pkt. 5.10.2 auf S. 118).
Die Aufgabe **Quarantäne untersuchen** entspricht der Aufgabe, die mit Hilfe der Schaltfläche **Alle untersuchen** im Fenster **Quarantäne** (s. Abbildung 50) gestartet werden kann.

- Wiederherstellen von Dateien in dem Ordner, aus dem sie in die Quarantäne verschoben wurden. Zur Wiederherstellung eines Objekts wählen Sie dieses in der Liste aus und klicken auf **Wiederherstellen**. Bei der Wiederherstellung von Objekten, die aus Archiven, Mail-Datenbanken und Dateien in Mail-Formaten unter Quarantäne gestellt wurden, ist Erweitertdie Angabe des Ordners erforderlich, in dem sie wiederhergestellt werden sollen.

Wir empfehlen Ihnen, nur Objekte mit dem Status *Fehlalarm*, *virusfrei* und *desinfiziert* wiederherzustellen, da die Wiederherstellung anderer Objekte zu einer Infektion Ihres Computers führen kann!

- Senden von möglicherweise infizierten Objekten zur Analyse an die Experten von Kaspersky Lab. Wir empfehlen Ihnen, Objekte nur dann zur Analyse einzusenden, wenn sich der Objektstatus *möglicherweise infiziert* auch nach mehrfachem Untersuchungs- und Desinfektionsversuch nicht geändert hat. Klicken dazu auf **Senden** (Details s. Anhang A auf S. 218).

Bitte beachten Sie, dass eine zum Senden vorgesehene Datei mit Kaspersky Anti-Virus untersucht worden sein muss, wobei die verwendeten Datenbanken nicht älter als einen Tag sein dürfen.

- Löschen eines beliebigen Objekts oder einer Gruppe ausgewählter Objekte aus Quarantäne. Löschen Sie nur jene Objekte, deren Desinfektion nicht möglich ist. Um Objekte zu löschen, wählen Sie diese in der Liste und klicken Sie auf **Löschen**.

5.10.1.3. Arbeit mit Backup

Immer vor dem Reparieren oder Löschen eines infizierten oder verdächtigen Objektes legt Kaspersky Anti-Virus davon eine Kopie im Backup an.

Im Bedarfsfall können Sie jedes Objekt wieder herstellen, wenn beispielsweise beim Reparieren Daten verloren gegangen sind oder das Objekt irrtümlich

gelöscht wurde oder Sie wollen noch mal mit aktualisierten Antiviren-Datenbanken eine Reparatur versuchen.

Die Arbeit mit Sicherheitskopien wird im Fenster **Backup** (s. Abbildung 51) verwaltet, das sich mit einem Klick auf den Hyperlink Backup auf der Registerkarte **Sicherheit** (s. Abbildung 2) des Programmhauptfensters öffnet.

Auf der Registerkarte **Sicherheit** (s. Abbildung 2) wird neben dem Hyperlink Backup in Klammern die Gesamtzahl der gespeicherten Sicherungskopien angegeben.

Im Backup-Fenster können Sie folgenden Aktionen ausführen:

- Objekte im gleichen Verzeichnis wieder herstellen, von wo sie in den Backup verschoben wurden, oder in einem Wiederherstellungs-Verzeichnis. Zur Wiederherstellung des Objektes wählen Sie es in der Liste aus und klicken Sie auf die Schaltfläche **Wiederherstellen**.

  Das Objekt wird aus der Sicherungskopie unter dem gleichen Namen wiederhergestellt, den es vor der Desinfektion besaß.

  Wenn am ursprünglichen Speicherort ein Objekt mit gleichem Namen vorhanden ist (Diese Situation kann eintreten, wenn ein Objekt wiederhergestellt wird, dessen Sicherheitskopie vor der Desinfektion angefertigt wurde), dann erscheint eine entsprechende Warnung auf dem Bildschirm. Sie können den Speicherort des wiederherzustellenden Objekts ändern oder es umbenennen.

- Löschen einer beliebigen Quarantäne-Datei oder einer Gruppe ausgewählter Dateien aus dem Backup. Um eine Datei zu löschen, wählen Sie sie in der Liste aus und klicken Sie auf die Schaltfläche **Löschen**.

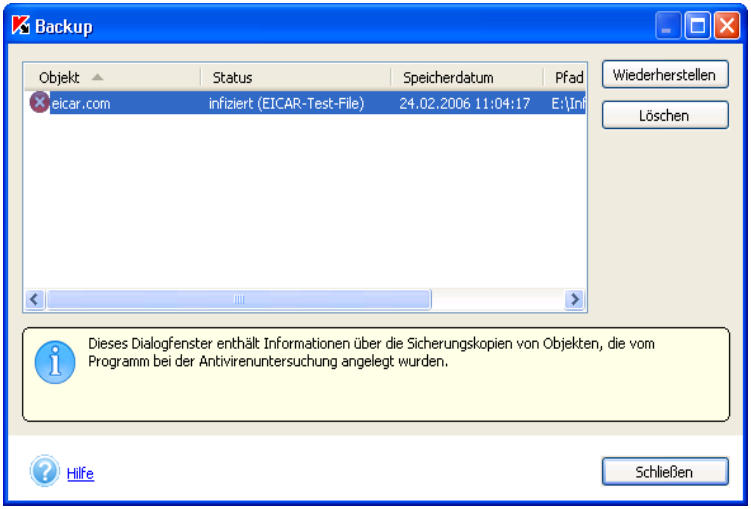

Abbildung 51. Backup-Fenster mit Sicherungskopien

Wann können Sicherungskopien wiederhergestellt werden?

Manchmal können Objekte bei der Desinfektion nicht vollständig repariert werden. Wenn eine desinfizierte Datei wichtige Informationen enthielt und diese aufgrund der Desinfektion vollständig oder teilweise nicht mehr zugänglich sind, kann versucht werden, das ursprüngliche Objekt aus der Sicherungskopie wiederherzustellen. Es wird empfohlen, das Objekt sofort nach der Wiederherstellung auf Viren zu untersuchen. Möglicherweise gelingt mit den aktualisierten Datenbanken die Desinfektion ohne Datenverlust.

Es wird davor gewarnt, Sicherungskopien von Objekten wiederherzustellen, wenn dies nicht unbedingt erforderlich ist. Dabei kann der Computer infiziert werden.

Standardmäßig sind die Speicherdauer für Sicherungskopien und die maximale Größe des Backup-Speichers unbegrenzt. Wir empfehlen Ihnen, den Speicher regelmäßig zu überprüfen und zu bereinigen. Außerdem stehen Optionen zur Verfügung, die es dem Programm erlauben, selbständig die ältesten Kopien zu löschen und Sie bei Überfüllung des Speichers zu benachrichtigen (Details s. Pkt. 5.10.1.1 auf S. 112).

5.10.2. Arbeit mit Protokollen

Während die Untersuchung des Computers, die Updates der Antiviren-Datenbanken und der Echtzeitschutz ausgeführt werden, werden ein Protokoll

über untersuchte Objekte und Behandlungsergebnisse sowie eine Gesamtstatistik erstellt.

Die vollständige Ergebnisliste aller ausgeführten Aufgaben wird von Kaspersky Anti-Virus im Fenster (s. Abbildung 52) geführt, das über den Hyperlink Protokolle im linken Teil der Registerkarte **Sicherheit** (s. Abbildung 2) geöffnet werden kann. Hier wird der Status für jede Aufgabe sowie das Datum und die Uhrzeit für den Abschluss eingestellt.

Angaben über die Verarbeitung des Objektes können mit folgenden Statusmeldungen gemacht werden:

- oder *Informatives Protokoll* enthält informative Angaben (z.B. Aufgabe wurde gestartet, Aufgabe wurde abgeschlossen, Aufgabe wird ausgeführt, Aufgabe wurde angehalten).
- *"Achtung"-Protokoll* enthält wichtige und kritische Informationen (z.B. Achtung! Es sind noch unbearbeitete Objekte vorhanden).
- *Hinweisprotokoll* kommentiert bestimmte wichtige Momente der Programmarbeit (z.B. Aufgabe wurde abgebrochen).

In der Regel besitzen Infoprotokolle begleitenden Charakter und sind nicht von vordringlicher Wichtigkeit. Sie können die Anzeige von Protokollen für die Aufgaben deaktivieren, in denen nur Daten vom Typ Meldungen vorkommen. Entfernen Sie dazu das Häkchen im Kontrollkästchen **Informative Protokolle anzeigen**. Beachten Sie, dass Protokolle über die laufende Ausführung einer bestimmten Aufgabe, die mit dem Symbol gekennzeichnet sind, immer angezeigt werden.

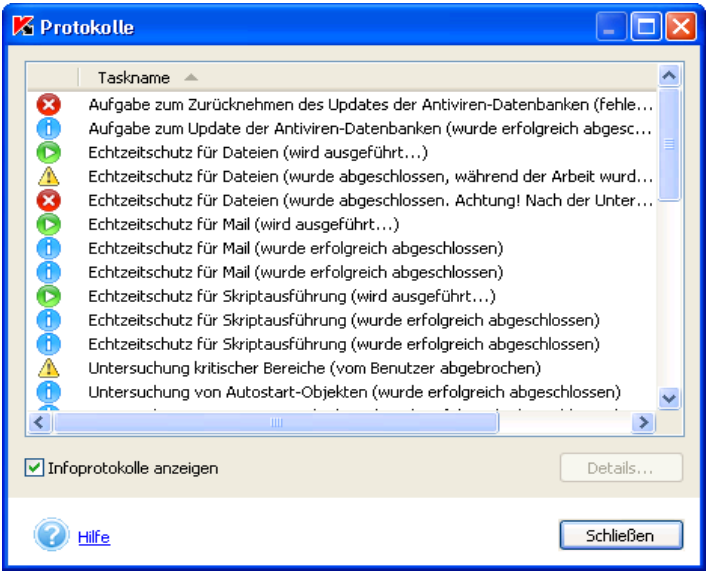
Protokolle
Taskname
Aufgabe zum Zurücknehmen des Updates der Antiviren-Datenbanken (fehle...
Aufgabe zum Update der Antiviren-Datenbanken (wurde erfolgreich abgesc...
Echtzeitschutz für Dateien (wird ausgeführt...)
Echtzeitschutz für Dateien (wurde abgeschlossen, während der Arbeit wurd...
Echtzeitschutz für Dateien (wurde abgeschlossen. Achtung! Nach der Unter...
Echtzeitschutz für Mail (wird ausgeführt...)
Echtzeitschutz für Mail (wurde erfolgreich abgeschlossen)
Echtzeitschutz für Mail (wurde erfolgreich abgeschlossen)
Echtzeitschutz für Skriptausführung (wird ausgeführt...)
Echtzeitschutz für Skriptausführung (wurde erfolgreich abgeschlossen)
Echtzeitschutz für Skriptausführung (wurde erfolgreich abgeschlossen)
Untersuchung kritischer Bereiche (vom Benutzer abgebrochen)
Untersuchung von Autostart-Objekten (wurde erfolgreich abgeschlossen)
Infoprotokolle anzeigen
Details...
Hilfe
Schließen

Abbildung 52. Fenster **Protokolle**

Hier ist außerdem das Sortieren der vorhandenen Protokolle nach Protokolltyp, Name (in alphabetischer Reihenfolge) oder im Protokoll enthaltener Abschlusszeit der Aufgabe möglich. Um die im Protokollfenster vorhandenen Protokolle nach einem der oben genannten Kriterien zu sortieren, klicken Sie mit der linken Maustaste auf die Überschrift der entsprechenden Spalte.

In diesem Fenster können Sie mit Hilfe der Befehle des Kontextmenüs (das durch Rechtsklick auf den Namen eines Protokolls geöffnet wird) folgende Aktionen ausführen:

- **Detail-Protokolll in Datei exportieren**. Geben Sie im folgenden standardmäßigen Microsoft Windows-Fenster einen Dateinamen an, wählen Sie einen Ordner auf einem Laufwerk, in dem diese Datei gespeichert werden soll und klicken Sie auf **Speichern**. Das Protokoll wird in Form einer Microsoft Excel Tabelle oder als Textdatei gespeichert.

- **Protokoll an Kaspersky Lab senden**. Sie können das Protokoll einsenden, wenn eine Aufgabe (beispielsweise die Untersuchung des Computers oder das Update der Antiviren-Datenbanken) abgebrochen oder fehlerhaft beendet wurde und Sie den Grund für dieses Verhalten des Programms nicht finden können. Durch Auswahl dieses Befehls wird automatisch das Fenster des auf Ihrem Computer standardmäßig verwendeten Mailprogramms geöffnet (z.B. Microsoft Outlook Express), in dem eine E-Mail-Nachricht mit der angehängten Protokolldatei erstellt

wird. Senden Sie diese E-Mail ab. Die Kaspersky-Lab-Spezialisten werden sich bemühen, Ihnen so schnell wie möglich zu helfen.

Das automatische Erstellen von E-Mail-Nachrichten funktioniert in den Mailprogrammen Microsoft Outlook und Microsoft Office Outlook Express. Wenn auf Ihrem Computer ein anderes Mailsystem (beispielsweise The Bat!) installiert ist, muss in Ihrem Mailprogramm die Unterstützung von Simple MAPI eingestellt werden, damit E-Mails automatisch erstellt werden.

- Mit Hilfe der Befehle **Löschen** oder **Alle löschen** ein Protokoll oder alle Protokolle aus der Liste entfernen. Ein Protokoll einer momentan laufenden Aufgabe kann nicht gelöscht werden.

Durch die Auswahl einer beliebigen Aufgabe im Journal können Sie deren Einstellungen, Statistik der Arbeitsergebnisse und Protokoll über gefundene Objekte auf den entsprechenden Registerkarten lesen. Klicken Sie dazu auf die Schaltfläche **Details**.

Im folgenden Fenster befindet sich auf den Registerkarten **Statistik**, **Protokoll** und **Einstellungen** für das Detail-Protokoll über die Aufgabenausführung.

Die Registerkarte **Statistik** (s. Abbildung 53) enthält allgemeine Informationen über die von Kaspersky Anti-Virus bei der Ausführung einer Aufgabe vorgenommene Arbeit: Datum und Uhrzeit von Aufgabenstart, Gesamtzahl der untersuchten Dateien, Anzahl der infizierten und reparierten Objekte sowie in Quarantäne gespeicherten Objekte. Für die Updateaufgabe werden auf der Registerkarte die Gesamtgröße der Updates an der Updatequelle und die Größe der auf den Computer heruntergeladenen Updates angezeigt.

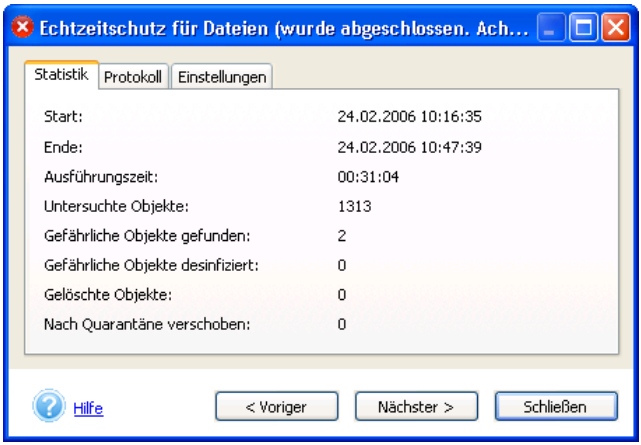

Abbildung 53. Registerkarte **Statistik**

Die Registerkarte **Protokoll** (s. Abbildung 55) enthält standardmäßig keine Informationen über virusfreie Objekte, sondern nur Informationen über gefundenen Viren. Zur Anzeige von Informationen über virusfreie Objekte muss in den erweiterten Einstellungen von Kaspersky Anti-Virus (s. Pkt. 5.10.4 auf S. 125) das Kontrollkästchen **Alle Protokolle speichern** aktiviert werden. In diesem Fall enthält die Registerkarte Informationen über jedes untersuchte Objekt. Für die Updateaufgabe enthält die Registerkarte Informationen über jeden Schritt: Verbindung mit der Updatequelle, heruntergeladene Dateien, Informationen über die Reihenfolge der Datei-Installation auf dem Computer. Die Informationen auf dieser Registerkarte sind immer vorhanden, unabhängig davon, ob das Kontrollkästchen **Alle Protokolle speichern** in den erweiterten Einstellungen von Kaspersky Anti-Virus aktiviert ist.

Damit während der laufenden Sitzung keine Informationsprotokolle angezeigt werden (ohne dabei das Kontrollkästchen **Alle Protokolle speichern** *zu deaktivieren),*

öffnen Sie während der Protokollanzeige auf der Registerkarte **Protokoll** (s. Abbildung 55) durch Rechtsklick das Kontextmenü (s. Abbildung 54) und deaktivieren Sie das Kontrollkästchen **Infoprotokolle anzeigen**.

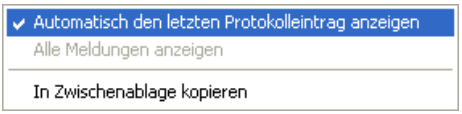

Abbildung 54. Kontextmenü für Protokolle

Außerdem können Sie Informationen über ein bestimmtes Ereignis in die Zwischenablage kopieren. Wählen Sie dazu das gewünschte Ereignis aus und verwenden Sie den Kontextmenübefehl **In Zwischenablage kopieren**.

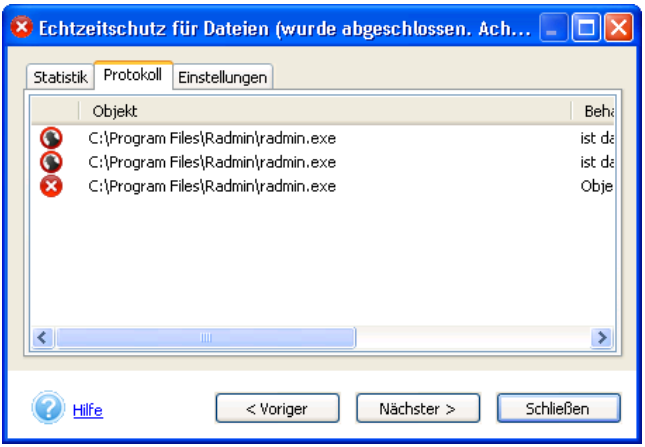

Abbildung 55. Registerkarte **Protokoll**

Auf der Registerkarte **Einstellungen** (s. Abbildung 56) sind die Parameter einer Aufgabe gespeichert, nach denen sie ausgeführt wurde. Hier werden Informationen über die Untersuchungsobjekte, die für diese Aufgabe festgelegte Sicherheitsstufe und die Programmaktionen für infizierte Objekte, schädliche Programme und verdächtige Dateien angezeigt.

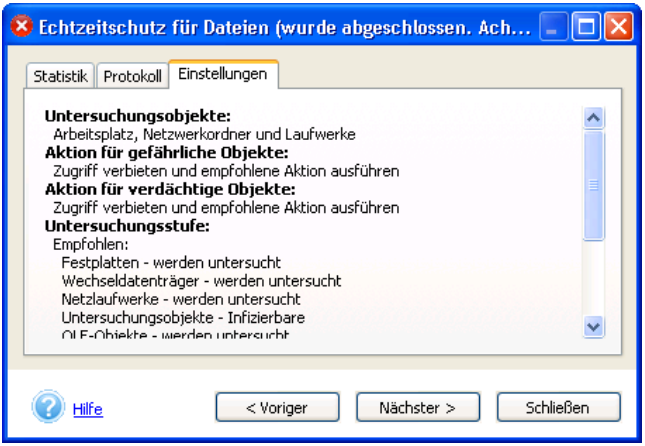

Abbildung 56. Registerkarte **Einstellungen**

Aufgaben können sowohl im Aufgabenjournal, als auch direkt im Fenster Detail-Protokolle mithilfe der Schaltflächen **Nächste** und **Vorige** sowie anhand des Aufgabennamens aus der sich öffnenden Liste zur Anzeige ausgewählt werden.

Die Einstellungen für die Optionen des Protokolljournals können Sie im Fenster **Zusatzeinstellungen** (s. Abbildung 58) vornehmen, das sich mit einem Klick auf den gleichnamigen Hyperlink im linken Teil der Registerkarte **Einstellungen** (Näheres siehe Punkt 5.10.4 auf S. 125) öffnet. Hier können Sie die maximal zulässige Aufbewahrungszeit für Protokolle bestimmen, Eintragungen in das Detail-Protokoll für diejenigen Meldungen zulassen/unterdrücken, die einen informativen Status besitzen.

5.10.3. Verwaltung der Konfiguration von Kaspersky Anti-Virus

Kaspersky Anti-Virus bietet Ihnen die Möglichkeit, unterschiedliche Konfigurationen für die Arbeit mit dem Programm zu erstellen und zu verwenden. Sie können einen bestimmten Modus der Programmfunktion konfigurieren, seine Parameter in einer speziellen Konfigurationsdatei (*Profil*) speichern und diese Konfiguration bei Bedarf verwenden.

Um zur Verwaltung der Programmkonfiguration zu wechseln, verwenden Sie den Hyperlink Profil-Verwaltung auf der linken Seite der Registerkarte **Einstellungen** (s. Abbildung 3).

Im folgenden Fenster (s. Abbildung 57) können Sie mit Hilfe der Schaltfläche **Profil speichern** die aktuellen Programmeinstellungen in einer speziellen Konfigurationsdatei speichern, oder mit der Schaltfläche **Profil laden** die Einstellungen einer zuvor für Kaspersky Anti-Virus erstellten Konfigurationsdatei übernehmen. In bestimmten Fällen kann nach dem Laden der Einstellungen der Neustart des Computers erforderlich sein, weil bestimmte Funktionsmodi beim Systemstart gestartet werden.

Klicken Sie auf **Profil wiederherstellen**, um die empfohlenen Funktionsparameter wiederherzustellen.

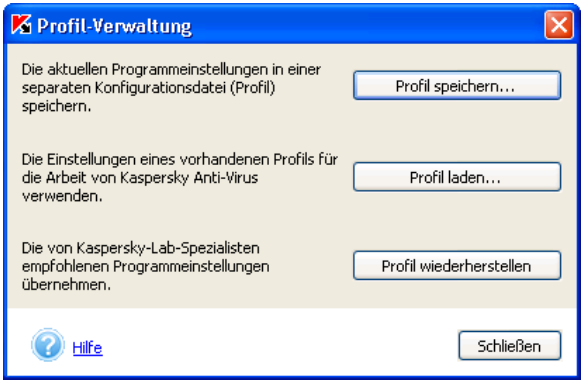
Profil-Verwaltung
Die aktuellen Programmeinstellungen in einer separaten Konfigurationsdatei (Profil) speichern.
Profil speichern...
Die Einstellungen eines vorhandenen Profils für die Arbeit von Kaspersky Anti-Virus verwenden.
Profil laden...
Die von Kaspersky-Lab-Spezialisten empfohlenen Programmeinstellungen übernehmen.
Profil wiederherstellen
Hilfe
Schließen

Abbildung 57. Profilverwaltung

5.10.4. Erweiterte Einstellungen

Neben der Konfiguration von Einstellungen konkreter Aufgaben bietet Kaspersky Anti-Virus auch die Möglichkeit, generelle und dienstbezogene Einstellungen anzupassen (s. Abbildung 58).

Um zu den erweiterten Einstellungen für Kaspersky Anti-Virus zu gelangen,

verwenden Sie den Hyperlink Erweiterte Einstellungen auf der linken Seite der Registerkarte **Einstellungen** (s. Abbildung 3). Dadurch gelangen Sie in das Fenster mit den Registerkarten **Allgemein**, **Leistung** und **Sicherheit**.

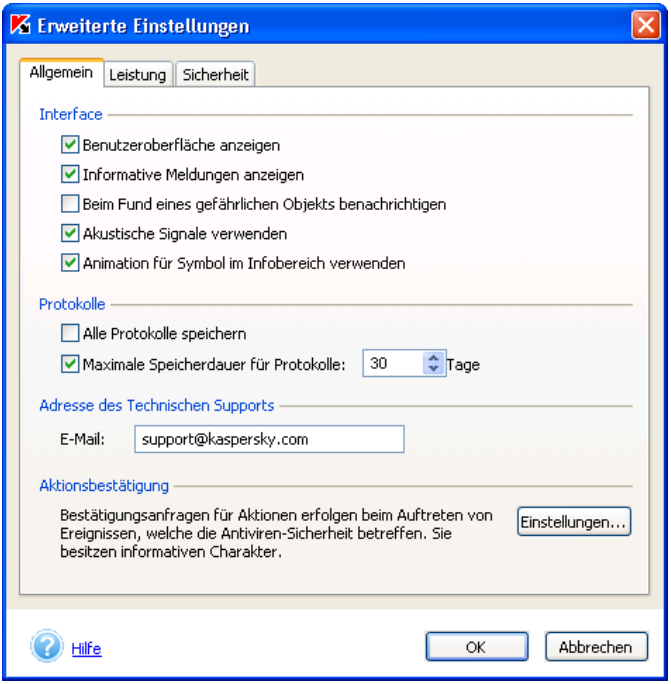

Abbildung 58. Erweiterte Einstellungen für Kaspersky Anti-Virus. Registerkarte **Allgemein**

Auf der Registerkarte **Allgemein** (s. Abbildung 58) können Sie folgende Einstellungen vornehmen:

- **Benutzeroberfläche anzeigen** – Aktivieren der Anzeige des Programmsymbols in der Taskleiste und Erlaubnis zur Anzeige des Hauptfensters der Anwendung im Benutzermodus (s. Pkt. 5.10.7 auf S. 131).

  Die Einstellungen, welche die Anzeige der Benutzeroberfläche betreffen, werden erst nach dem Neustart des Computers wirksam.

- **Informative Meldungen anzeigen** – Aktivieren der Bildschirmanzeige aller Meldungen, welche die Arbeit von Kaspersky Anti-Virus begleiten. Die Meldungen werden über dem Programmsymbol in der Taskleiste eingeblendet.

  Die Anzeige von Meldungen steht bei der Arbeit mit den Betriebssystemen Microsoft Windows 98 und Microsoft Windows NT Workstation 4.0 nicht zur Verfügung.

- **Beim Fund eines gefährlichen Objekts benachrichtigen** – Aktivieren der Anzeige von Benachrichtigungen über den Fund gefährlicher Objekte.
- **Akustische Signale verwenden** – Aktivieren der Wiedergabe bestimmter akustischer Signale beim Eintreten von Ereignissen während der Arbeit von Kaspersky Anti-Virus. Zur Anzeige einer Liste der Ereignisse und zum Ändern der entsprechenden Audiodateien können die Mittel des Betriebssystems Microsoft Windows verwendet werden (**Start → Einstellungen → Systemsteuerung → Sounds und Audiogeräte → Sounds**).
- **Animation für Symbol im Infobereich verwenden** – Animation des Symbols in Abhängigkeit der von Kaspersky Anti-Virus ausgeführten Operation. Bei der Untersuchung einer E-Mail erscheint über dem Symbol beispielsweise ein blinkender Briefumschlag.
- **Alle Protokolle speichern** – Das Speichern aller Protokolle, die während der Arbeit des Programms erstellt werden, wird aktiviert: Meldungen mit informativem Charakter, Fehlermeldungen usw. Dieser Modus ist standardmäßig deaktiviert und es werden lediglich wichtige Meldungen aufgezeichnet (beispielsweise fehlerhafter Abschluss des Programms, Abbruch der Aufgabenausführung usw.).
- **Maximale Speicherdauer für Protokolle ... (Tage)**. Standardmäßig beträgt die Speicherdauer für Protokolle 30 Tage. Sie können die Speicherdauer ändern, indem Sie im rechts angebrachten Feld einen anderen Wert festlegen, oder die Begrenzung aufheben, indem Sie das Kontrollkästchen deaktivieren. Die Kontrolle der Speicherdauer von Protokollen und das Löschen veralteter Protokolle erfolgt beim Start von Anti-Virus.

Im Abschnitt **Adresse des Technischen Supports** können Sie die Adresse des technischen Kundendiensts angeben. Standardmäßig steht hier die E-Mail-Adresse des technischen Support-Service von Kaspersky Lab (support@kaspersky.com). Sie können in diesem Feld beispielsweise die E-Mail-Adresse des Sicherheitsadministrators oder die Adresse einer Webseite angeben, die bei einer Anfrage an den technischen Kundendienst geöffnet werden soll.

Im Abschnitt **Aktionsbestätigung** wird die Anzeige der Eingabeaufforderungen angepasst, die Kaspersky Anti-Virus bei bestimmten Ereignissen während seiner Arbeit auf dem Bildschirm anzeigt. In der Regel besitzen alle Eingabeaufforderungen informativen Charakter. Details über die Optionen für Bestätigungsanfragen finden Sie unter Pkt. 5.10.5 auf S. 130.

Auf der Registerkarte **Leistung** (s. Abb. 59) können Sie Beschränkungen festlegen, die für den Scan auf Befehl gelten sollen, um bei Batterieversorgung (bei der Arbeit mit einem Notebook) für ökonomischen Stromverbrauch und

Umgang mit Betriebssystemressourcen zu sorgen (Details s. Pkt. 5.10.6 auf S. 131).

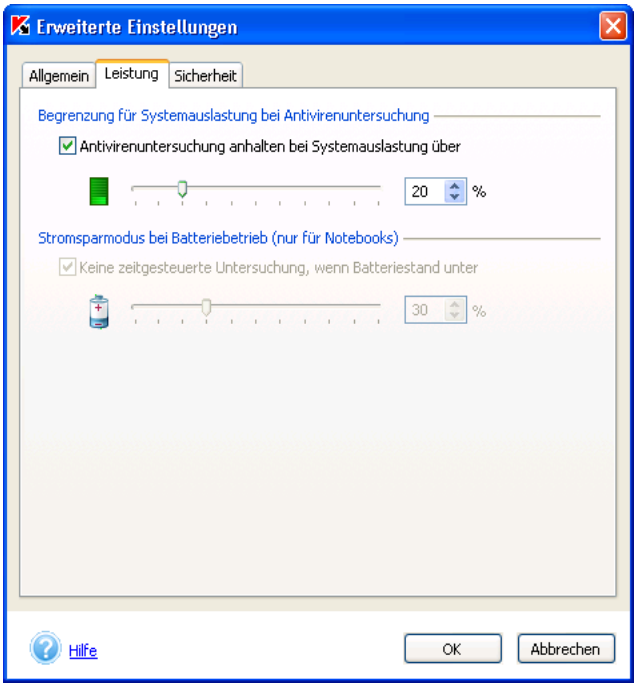

Abbildung 59. Erweiterte Einstellungen für Kaspersky Anti-Virus. Registerkarte **Leistung**

Die Registerkarte **Sicherheit** (s. Abbildung 61) enthält folgende Einstellungen:

- **Kaspersky Anti-Virus bei Systemstart starten** – Aktivieren des Starts von Kaspersky Anti-Virus nach dem Neustart des Betriebssystems.

  Wir empfehlen Ihnen ausdrücklich, die Arbeit von Kaspersky Anti-Virus nicht zu deaktivieren, weil dies zu einer Infektion Ihres Computers führen kann.

  Diese Option steht nur zur Verfügung, wenn Sie auf dem Computer über Administratorrechte verfügen.

- **System zur Wiederherstellung nach Störungen verwenden** – Das Wiederherstellungssystem für die Arbeit von Kaspersky Anti-Virus beim Auftreten von Störungen wird aktiviert. Wenn die Funktion der Anwendung gestört wurde, wird das Hauptfenster von Kaspersky Anti-Virus geschlossen (falls es geöffnet war) und über dem Symbol im

Infobereich der Taskleiste erscheint ein Hinweis (s. Abbildung 60). Danach wird die Arbeit der Anwendung automatisch wiederhergestellt.

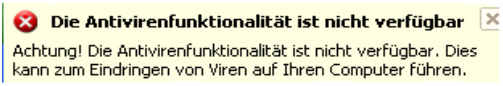
Die Antivirenfunktionalität ist nicht verfügbar
Achtung! Die Antivirenfunktionalität ist nicht verfügbar. Dies kann zum Eindringen von Viren auf Ihren Computer führen.

Abbildung 60. Störung bei der Arbeit der Anwendung

Kennwort zum Programmschutz verwenden – Aktivieren der Kennwortabfrage beim Wechsel vom Administratormodus in den Benutzermodus. Die Verwendung dieses Modus wird empfohlen, wenn außer Ihnen noch ein anderer Benutzer Zugang zu Ihrem Computer hat und Sie nicht möchten, dass dieser die Antivirenschutzeinstellungen ändern, den Echtzeitschutz deaktivieren und Kaspersky Anti-Virus beenden kann (Details s. Pkt. 5.10.7 auf S. 131). Wurde dieser Modus aktiviert, dann geben Sie im Feld **Kennwort** ein Kennwort ein und bestätigen Sie das Kennwort im Feld **Kennwort bestätigen**.

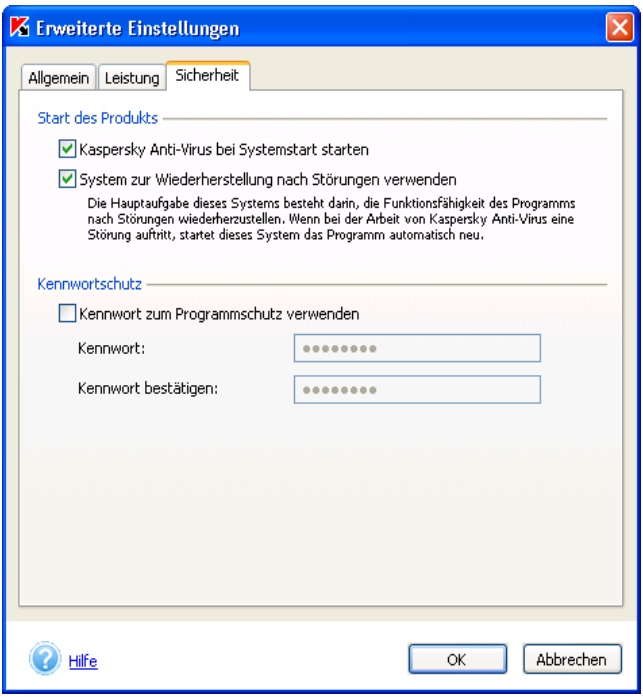
Erweiterte Einstellungen
Allgemein
Leistung
Sicherheit
Start des Produkts
Kaspersky Anti-Virus bei Systemstart starten
System zur Wiederherstellung nach Störungen verwenden
Die Hauptaufgabe dieses Systems besteht darin, die Funktionsfähigkeit des Programms nach Störungen wiederherzustellen. Wenn bei der Arbeit von Kaspersky Anti-Virus eine Störung auftritt, startet dieses System das Programm automatisch neu.
Kennwortschutz
Kennwort zum Programmschutz verwenden
Kennwort:
Kennwort bestätigen:
Hilfe
OK
Abbrechen

Abbildung 61. Erweiterte Einstellungen für Kaspersky Anti-Virus. Registerkarte **Sicherheit**

5.10.5. Einstellungen für Eingabeaufforderungen

Wenn Sie während der Arbeit des Programms über bestimmte Ereignisse informiert werden möchten, verwenden Sie den Hyperlink Erweiterte Einstellungen auf der linken Seite der Registerkarte **Einstellungen** (s. Abbildung 3). Klicken Sie im Fenster für erweiterte Einstellungen im Abschnitt **Aktionsbestätigung** auf die Schaltfläche **Einstellungen**. Dadurch gelangen Sie in das Fenster zum Anpassen der Hinweise (s. Abbildung 62).

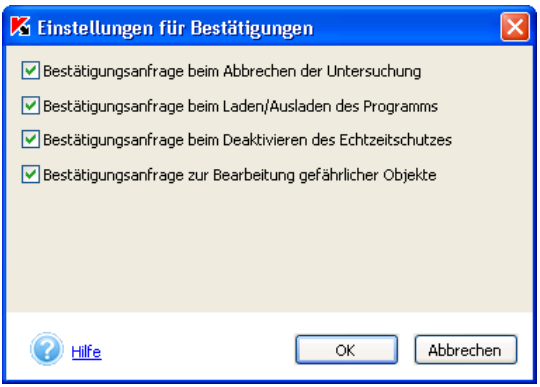

Abbildung 62. Anpassen der Eingabeaufforderungen

Folgende Ereignisse sind vorgesehen:

- **Eingabeaufforderung beim Abbrechen der Untersuchung** – Auf dem Bildschirm erscheint eine Anfrage, durch die das Abbrechen des Scan auf Befehl bestätigt werden kann. Nach dem Abbruch der Untersuchung erscheint über dem Programmsymbol im Systemschacht ein Popuphinweis, der die Gründe für das Abbrechen der Untersuchung nennt.
- **Eingabeaufforderung beim Laden/Ausladen des Programms** – Auf dem Bildschirm erscheint eine Anfrage, zur Bestätigung des Starts bzw. des Beendens von Kaspersky Anti-Virus.
- **Eingabeaufforderung beim Deaktivieren des Echtzeitschutzes** – Wenn der Schutz Ihres Computers in den Echtzeitschutz-Einstellungen vollständig deaktiviert wird, erscheint eine entsprechende Warnung auf dem Bildschirm. Dieses Kontrollkästchen ist nicht verfügbar, wenn Sie bei der Installation von Kaspersky Anti-Virus die Verwendung des Datei-Echtzeitschutzes abgelehnt haben.

- **Eingabeaufforderung zur Bearbeitung gefährlicher Objekte** – Es erfolgt eine Meldung darüber, dass aufgrund der Untersuchung noch unbearbeitete infizierte Objekte vorhanden sind.

5.10.6. Beschränkungen der Leistung von Kaspersky Anti-Virus

Sie können festlegen, dass Kaspersky Anti-Virus die Untersuchung nicht startet, wenn die Verwendung von Computerressourcen eingeschränkt werden muss. Verwenden Sie dazu auf der linken Seite der Registerkarte **Einstellungen** (s. Abbildung 3) den Hyperlink Erweiterte Einstellungen. Gehen Sie im folgenden Fenster auf die Registerkarte **Leistung** (s. Abbildung 59).

Folgende Beschränkungen sind möglich:

- **Antivirenuntersuchung anhalten bei Systemauslastung über …%** – Der Scan auf Befehl wird angehalten, wenn die Auslastung des Dateisystems über das festgelegte Niveau steigt. Sobald die Auslastung des Dateisystems auf das zulässige Niveau sinkt, wird die Untersuchung fortgesetzt. Legen Sie mit Hilfe des Schiebereglers oder im rechts angebrachten Feld einen Wert für die maximal zulässige Systemauslastung (in Prozent) fest, bei dessen Überschreitung die zeitgesteuerte Untersuchung nicht ausgeführt werden soll.

  Dieser Parameter ist nur für den Scan auf Befehl (beispielsweise Untersuchung eines ausgewählten Objekts) gültig. Der Echtzeitschutz wird dadurch nicht beeinflusst.

- **Stromsparmodus bei Batteriebetrieb (nur für Notebooks) ...%** – Bei der Arbeit auf einem Notebook wird der Start des Scan auf Befehl nicht ausgeführt, wenn der Ladestand des Akkumulators unter dem festgelegten Wert liegt. Legen Sie mit Hilfe des Schiebereglers oder im rechts angebrachten Feld einen Wert für den zulässigen Akkuladestand (in Prozent) fest, bei dessen Unterschreitung die zeitgesteuerte Untersuchung nicht gestartet werden soll.

  Diese Option ist nur verfügbar, wenn Kaspersky Anti-Virus auf einem Notebook installiert ist und die Stromversorgung über Akkumulator erfolgt.

5.10.7. Arbeit im Administrator- und Benutzermodus

Kaspersky Anti-Virus kann im Administratormodus und im Benutzermodus arbeiten. Die Verwendung dieser Modi kann nützlich sein, wenn außer Ihnen noch ein anderer Benutzer Zugriff auf Ihren Computer besitzt. Sie können diesem Benutzer verbieten, die Einstellungen des Antivirenschutzes zu ändern,

den Echtzeitschutz zu deaktivieren und Kaspersky Anti-Virus zu beenden. Im Benutzermodus verändert sich die Programmoberfläche, die gesperrten Einstellungen werden ausgeblendet (zum Beispiel wird die Registerkarte **Einstellungen** im Programmhauptfenster nicht angezeigt).

Die Verwendung des Benutzer- und Administratormodus kann über das lokale Interface und mit Hilfe der Anwendung Kaspersky Administration Kit aktiviert werden (s. Pkt. 6.2.2.14 auf S. 167).

Um die Verwendung des Benutzer- und Administratormodus über das lokale Interface zu aktivieren,

aktivieren Sie das Kontrollkästchen **Kennwort zum Programmschutz verwenden** auf der Registerkarte (s. Abbildung 61) im Fenster der erweiterten Einstellungen von Kaspersky Anti-Virus. Geben Sie das Kennwort im Feld **Kennwort** an und bestätigen Sie es im Feld **Kennwort bestätigen**.

Danach erscheint im Kontextmenü des Programms (s. Abbildung 1) der Befehl **In den Benutzermodus wechseln**, mit dessen Hilfe Sie in den Benutzermodus wechseln können. Um zum Administratormodus zurückzukehren verwenden Sie den Kontextmenübefehl **In den Administratormodus wechseln** und geben Sie im folgenden Fenster (s. Abbildung 63) das Kennwort an.

Wenn das Kontrollkästchen **Kennwort zum Programmschutz verwenden** (s. Abbildung 61) nicht aktiviert ist, erfolgen Start und Arbeit von Kaspersky Anti-Virus im Administratormodus.

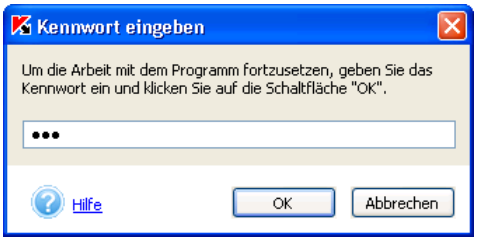
Kennwort eingeben
Um die Arbeit mit dem Programm fortzusetzen, geben Sie das Kennwort ein und klicken Sie auf die Schaltfläche "OK".
Hilfe
OK
Abbrechen

Abbildung 63. Kennworteingabe

Um die Anwendungsoberfläche im Benutzermodus vollständig auszublenden,

deaktivieren Sie das Kontrollkästchen **Benutzeroberfläche anzeigen** auf der Registerkarte **Allgemein** (s. Abbildung 58) im Fenster der erweiterten Einstellungen für Kaspersky Anti-Virus.

In diesem Fall wird im Benutzermodus das Symbol von Kaspersky Anti-Virus nicht in der Taskleiste angezeigt und das Programmhauptfenster wird nicht geöffnet.

KAPITEL 6. BEDIENUNG DER ANWENDUNG MIT KASPERSKY ADMINISTRATION KIT

6.1. Bedienung mit Installationspaketen

Dieser Abschnitt enhält Informationen über das Erstellen und die Konfiguration eines Installationspakets für Kaspersky Anti-Virus 5.0 for Windows Workstations. Einzelheiten über die Konzeption zur Steuerung mit Installationspaketen finden Sie im Administratorhandbuch für Kaspersky Administration Kit 5.0.

6.1.1. Erstellen eines Installationspakets

Gehen Sie folgendermaßen vor, um ein Installationspaket zu erstellen:

1. Melden Sie sich am erforderlichen Administrationsserver an.
2. Wählen Sie in der Konsolenstruktur das Element **Remote-Installation**, öffnen Sie das Kontextmenü und wählen Sie den Befehl **Neu** / **Installationspaket** oder verwenden Sie den entsprechenden Punkt im Menü **Aktion**. Folgen Sie den Anweisungen des dadurch gestarteten Assistenten.

Die Oberfläche des Programms zur Richtlinienerstellung besitzt die Form eines Assistenten für Microsoft Windows (Windows Wizard) und besteht aus einer Folge von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **< Zurück** und **Weiter >**. Die Arbeit des Assistenten wird mit der Schaltfläche **Fertig stellen** abgeschlossen. Mit Hilfe der Schaltfläche **Abbrechen** kann der Assistent auf einer beliebigen Etappe abgebrochen werden.

Beim Erstellen eines Installationspakets wird eine minimale Auswahl von Parametern festgelegt. Für die übrigen Parameter gelten Standardwerte, die

auch für die lokale Installation der Anwendung gelten. Die Parameter des Installationspakets können angepasst werden (s. Pkt. 6.1.2 auf S. 136).

Schritt 1. Angabe des Namens des Installationspakets

Das erste Fenster des Assistenten dient der Angabe des Namens des Installationspakets (Feld **Name**).

Schritt 2. Verbindung der Beschreibungsdatei des Installationspakets

Im folgenden Fenster des Assistenten wird die Anwendung für die Installation angegeben (s. Abb. 64). Wählen Sie in der Dropdown-Liste folgende Variante aus: **Kaspersky-Lab-Anwendungspaket erstellen** und wählen Sie mit Hilfe der Schaltfläche **Durchsuchen** die Datei mit der Beschreibung der Anwendung (diese Datei besitzt die Endung **.kpd** und gehört zur Distribution von Kaspersky Anti-Virus 5.0 for Windows Workstations). Dadurch werden automatisch die Felder mit dem Anwendungsnamen und der Versionsnummer ausgefüllt.

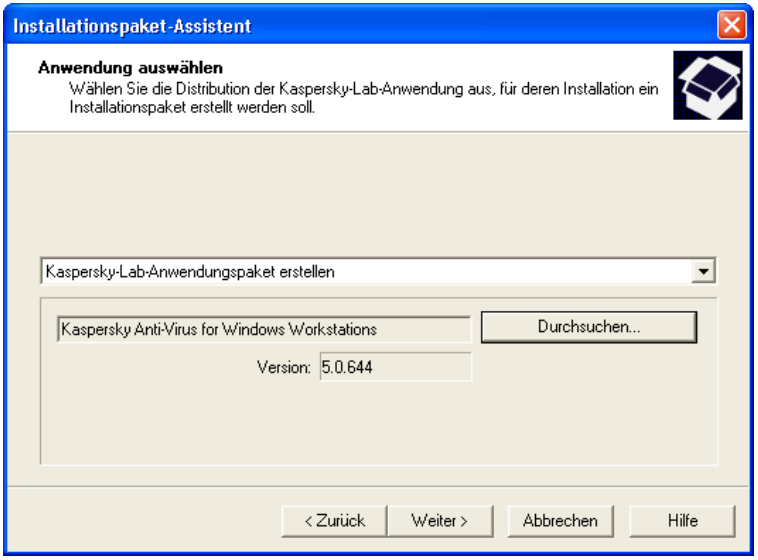

Abbildung 64. Erstellen eines Installationspakets. Auswahl der Anwendung für die Installation

Schritt 3. Auswahl der Lizenzschlüsseldatei

Im folgenden Fenster des Assistenten (s. Abb. 65) können Sie den Lizenzschlüssel wählen, der in das Installationspaket aufgenommen werden soll. Klicken Sie dazu auf die Schaltfläche **Durchsuchen** und wählen Sie die gewünschte Lizenzschlüsseldatei (diese Datei besitzt die Endung **.key**).

Wenn Sie keinen Lizenzschlüssel in das Installationspaket aufnehmen möchten, klicken Sie auf die Schaltfläche **Weiter**.

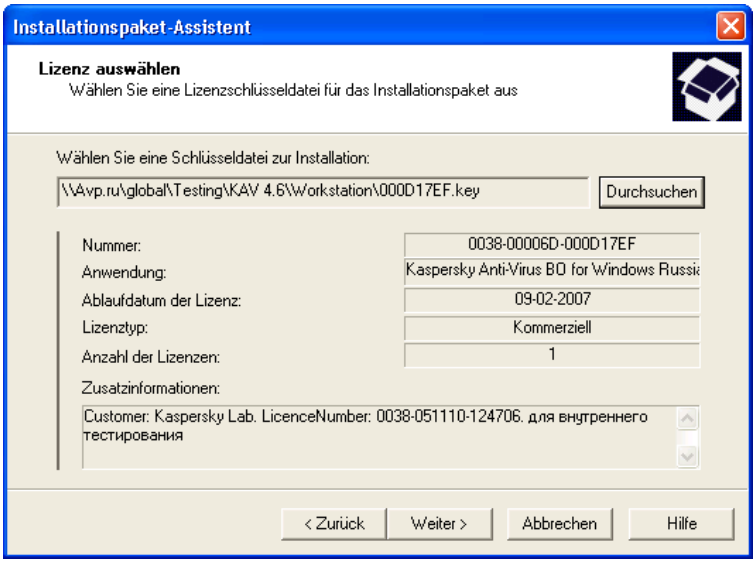

Abbildung 65. Erstellen eines Installationspakets. Auswahl des Lizenzschlüssels

Schritt 4. Abschluss des Erstellens eines Installationspakets

Klicken Sie im Fenster **Laden des Installationspakets** auf die Schaltfläche **Weiter**.

Danach wird die Auswahl der Dateien, die für die Installation der festgelegten Anwendung auf Client-Computern erforderlich sind, auf den Administrationsserver in den gemeinsamen Ordner geladen und es wird überprüft, ob das Verwaltungsplugin für die gewählte Anwendung am Administratorarbeitsplatz vorhanden ist. Wenn das Plugin nicht installiert ist oder eine ältere Version besitzt, als das in der Distribution vorhandene, wird es installiert oder ersetzt.

Das nächste Fenster des Assistenten enthält Informationen über den erfolgreichen Prozess zum Erstellen des Installationspakets. Das erstellte Installationspaket wird dem Element **Remote-Installation** hinzugefügt und erscheint in der Ergebnisleiste.

6.1.2. Anzeige und Ändern von Parametern eines Installationspakets

Um die Werte von Parametern eines Installationspakets anzuzeigen und/oder Änderungen darin vorzunehmen:

1. Wählen Sie in der Konsolenstruktur im Ordner **Remote-Installation** das Installationspaket aus, dessen Einstellungen Sie anpassen möchten.
2. Öffnen Sie das Kontextmenü der ausgewählten Richtlinie und verwenden Sie den Befehl **Eigenschaften**. Auf dem Bildschirm erscheint das Konfigurationsfenster der Richtlinie für **Kaspersky Anti-Virus 5.0 for Windows Workstations**, das mehrere Registerkarten enthält.

Das Fenster **Eigenschaften von <Name des Installationspakets>** besteht aus folgenden Registerkarten: **Allgemein**, **Installationseinstellungen**, **Lizenzdaten** und **Neustart des Betriebssystems**.

Die Registerkarten **Allgemein**, **Lizenzdaten** und **Neustart des Betriebssystems** sind standardmäßige Registerkarten für die Anwendung Kaspersky Administration Kit (Details s. Handbuch für Kaspersky Administration Kit 5.0).

Die Registerkarte **Installationseinstellungen** (s. Abb. 66) enthält Einstellungen für Kaspersky Anti-Virus5.0 for Windows Workstations:

- **Installationsordner** der Anwendung auf dem Client-Computer. Wenn dieses Feld leer bleibt, erfolgt die Installation in den standardmäßigen Ordner: **<Laufwerk>\Programme\Kaspersky Lab\Kaspersky Anti-Virus 5.0 for Windows Workstations**.
- **Kaspersky-Lab-Technologien zum Datenschutz**. Aktivieren Sie die Kontrollkästchen neben den Bezeichnungen der Schutz-Technologien, die Sie verwenden möchten.

Wenn Sie eine der genannten Technologien deaktivieren, muss zur späteren Aktivierung der Technologie die Anwendung auf dem Client-Computer neu installiert werden.

- **Kennwort für das Löschen** – Kennwort, das bei der Programmdeinstallation abgefragt wird. Geben Sie das Kennwort im entsprechenden Feld an und wiederholen Sie es im Feld **Kennwort bestätigen**.
- **Kennwort zum Programmschutz** – Kennwort für den Wechsel vom Benutzermodus in den Administratormodus. Geben Sie das Kennwort im entsprechenden Feld an und wiederholen Sie es im Feld **Kennwort wiederholen**.

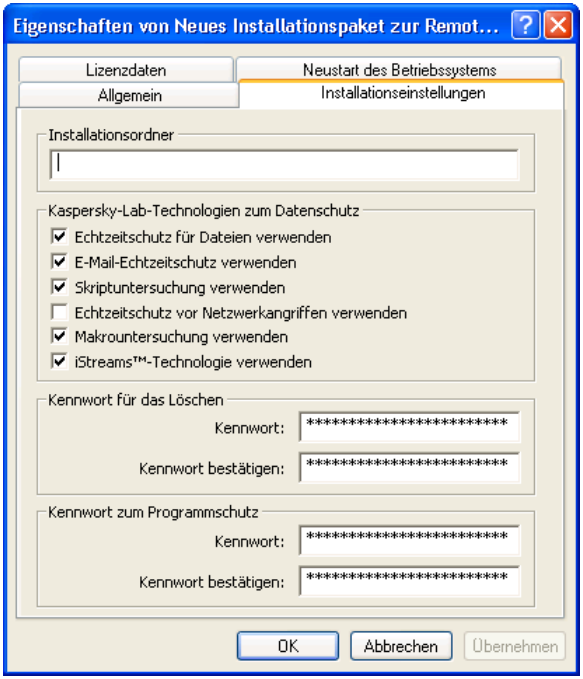

Abbildung 66. Eigenschaften des Installationspakets. Registerkarte **Installationsparameter**

6.2. Bedienung mit Richtlinien

In diesem Abschnitt werden die Anlage und Erstellung von Richtlinien für Kaspersky Anti-Virus 5.0 for Windows Workstations behandelt. Details zum Konzept der Bedienung mit Richtlinien finden Sie im Handbuch für den Systemadministrator Kaspersky Administration Kit 5.0.

6.2.1. Anlegen einer Richtlinie

Um eine Richtlinie anzulegen, gehen Sie wie folgt vor:

1. In der Konsole wählen Sie im Element **Gruppen** die Computergruppe aus, für die Sie eine Richtlinie anlegen wollen.
2. Wählen Sie den Ordner **Policy,** der zur ausgewählten Gruppe gehört und rufen Sie das Kontextmenü mit dem Befehl **Neu→Policy…** auf. Auf dem Bildschirm erscheint das Fenster für die Anlage einer neuen Richtlinie.

Die Programmschnittstelle für die Anlage einer Richtlinie entspricht dem Stil von Microsoft Windows-Assistenten (Windows Wizard) und besteht aus aufeinander folgenden Fenstern (Schritten), zu denen Sie mithilfe der Schaltflächen **< Zurück** und **Weiter >** und hin- und hergehen können und mit der Schaltfläche **Fertig** beenden. Um die Arbeit des Programm-Masters an beliebiger Stelle abzubrechen, klicken Sie auf die Schaltfläche **Abbrechen**.

Beim Erstellen einer Richtlinie wird nur eine minimale Auswahl von Parametern angepasst, die für die Funktion der Anwendung erforderlich sind. Die übrigen Werte werden standardmäßig festgelegt und entsprechen den standardmäßigen Werten bei der lokalen Installation der Anwendung. Sie können die die Richtlinie anpassen (s. Pkt. 6.2.2 auf S. 142).

Beim Anlegen einer Richtlinie (Schritt 2 - Schritt 5) können Sie unterbinden, dass Einstellungen von in Gruppen eingebetteten Richtlinien, eines Programms und von Aufgaben geändert werden. Um die Umschreibung der Einstellungen zu verhindern, aktivieren Sie für sie das „Schloss“: . Einstellungen, die geändert werden dürfen, sind so gekennzeichnet .

Schritt 1. Allgemeine Angaben zur Richtlinie

Die ersten Fenster des Assistenten dienen der Eingabe. Es müssen hier der Name der Richtlinie (Feld **Name**) eingegeben und die Anwendung **Kaspersky Anti-Virus 5.0 for Windows Workstations** in der Dropdownliste **Name der Anwendung** ausgewählt werden. Damit die zu erstellende Richtlinie als aktive Richtlinie für die Anwendung benutzt wird, aktivieren Sie die Richtlinie. Aktivieren Sie dazu im entsprechenden Fenster des Assistenten das Kontrollkästchen **Richtlinie aktivieren**.

In einer Gruppe können für eine Anwendung mehrere Richtlinien mit unterschiedlichen Parameterwerten erstellt werden. Allerdings kann nur eine Richtlinie für eine Anwendung gültig sein. Es besteht die Möglichkeit, eine ungültige Richtlinie bei Eintritt eines Ereignisses zu aktivieren. So können beispielsweise während einer Virusepidemie strengere Parameter für den Antivirenschutz wirksam gemacht werden.

Schritt 2. Auswahl der Sicherheitsstufe für Echtzeitschutz

Auf dieser Seite muss die Sicherheitsstufe des Antivirenschutzes ausgewählt werden, mit dem die Aufgaben des Echtzeitschutzes ausgeführt werden.

Schritt 3. Auswahl der Sicherheitsstufe für Scan auf Befehl

Auf dieser Seite muss die Sicherheitsstufe des Antivirenschutzes ausgewählt werden, mit dem ein Scan auf Befehl ausgeführt wird. Außerdem werden hier die Aktionen festgelegt, die beim Fund eines infizierten oder verdächtigen Objekts ausgeführt werden sollen (s. Pkt. 5.3.3.2 auf S. 88).

Mit einem Klick auf **Details** öffnet sich das Fenster mit detaillierten Einstellungen für den Scan auf Befehl. Wenn Einstellungen geändert werden, wechselt die Sicherheitsstufe in **Benutzereinstellungen**.

Schritt 4. Update-Quelle auswählen

Auf dieser Seite (s. Abbildung 67) werden die Optionen für den Update-Service der Antiviren-Datenbanken und der Programmmodule eingestellt: Update-Quelle angeben und Optionen des Lokalnetzes im Fenster angeben, das sich mit einem Klick auf die Schaltfläche **LAN-Einstellungen** öffnet. Alle Einstellungen gleichen den lokalen Einstellungen. Näheres dazu finden Sie in Punkt 5.1.3 auf S. 46.

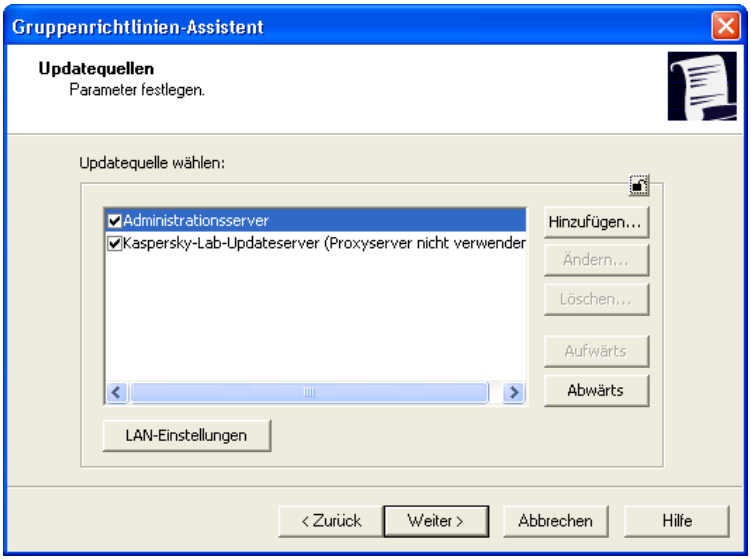

Abbildung 67. Update-Quelle auswählen

Schritt 5. Optionen für Update-Service

In diesem Fenster (s. Abbildung 68) werden die Optionen für den Dienst für Updates und Anwendungsmodule ausgewählt. Die Einstellungen für den Update-Vorgang gleichen den lokalen Einstellungen. Näheres dazu finden Sie unter Punkt 5.1.3 auf S. 46.

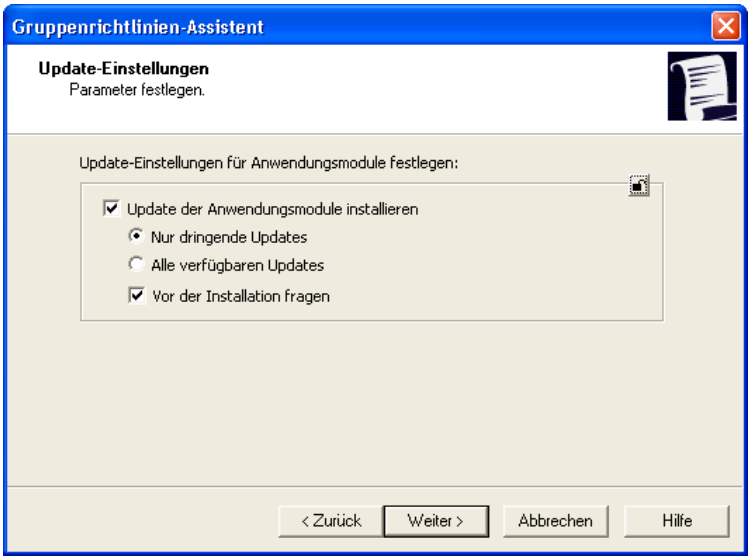

Abbildung 68. Optionen für Update-Service

Schritt 6. Abschluss des Erstellens der Richtlinie

Im letzten Fenster des Assistenten werden Sie informiert, dass die Anlage einer Richtlinie erfolgreich abgeschlossen wurde.

Nach Beendigung der Arbeit des Assistenten wird die Richtlinie für die gegebene Anwendung in den Ordner **Policy** der entsprechenden Gruppe eingefügt und in der Ergebnisliste angezeigt.

Für die Anwendung der Richtlinie bearbeiten Sie ihre Einstellungen und bestimmen Sie die Einschränkungen für die Änderungen der Aufgaben- und Anwendungseinstellungen, wenn Sie das nicht schon in dem Schritt Anlage der Richtlinie getan haben. An die Computer-Clients wird die Richtlinie bei der ersten Synchronisation der Clients mit dem Administrationsserver weiter gegeben.

Die Richtlinie wird folgenderweise angewendet: werden an einem Client residente Aufgaben (Echtzeitschutz) ausgeführt, dann übernehmen sie dazu die neuen Einstellungen. Regelmäßig gestartete Aufgaben (Scan auf Befehl, Update der Antiviren-Datenbanken) arbeiten mit den alten Einstellungen, beim erneuten Start werden die geänderten Einstellungen übernommen. Die Optionswerte für das Programm nach Wirksamkeit einer Richtlinie können Sie im Eigenschaften-Fenster des Clients unter **Eigenschaften von <Computername>** auf den Registerkarten **Anwendungen** und **Tasks** anzeigen lassen. Sie können Richtlinien von einer Gruppe in eine andere Gruppe kopieren und übertragen, sie

mit Standardbefehlen des Kontextmenüs **Kopieren/Einfügen**, **Ausschneiden/Einfügen** und **Löschen** oder den gleichen Punkten im Menü **Aktion** löschen. Ein Verschiebevorgang kann auch mithilfe der Maus erledigt werden.

6.2.2. Anzeige und Bearbeitung von Richtlinien-Optionen

In der Bearbeitungsphase können Sie eine Richtlinie ändern, die Änderung von Optionen in Richtlinien, die in Gruppen eingebettet sind, und die Einstellungen des Programms und von Aufgaben untersagen.

Um eine neue Einstellung zu verhindern, aktiveren Sie das „Schloss“: . Optionen, die geändert werden können, sind so gekennzeichnet .

Um die Optionswerte einer Richtlinie anzuzeigen und / oder zu ändern:

1. In der Konsole wählen Sie im Ordner **Gruppen** die Computergruppe aus, für die Sie die Einstellungen bearbeiten wollen.
2. Wählen Sie den zu dieser Gruppe gehörenden Ordner **Policy**, dabei werden in der Ergebnisliste alle für die Gruppe angelegten Richtlinien angezeigt.
3. In der Richtlinienliste stellen Sie den Mauszeiger auf die Richtlinie für die Anwendung **Kaspersky Anti-Virus 5.0 for Windows Workstations** (Name der Anwendung erscheint im Feld **Anwendungen**).
4. Rufen Sie das Kontextmenü der ausgewählten Richtlinie auf und gehen Sie auf den Befehl **Eigenschaften**, auf dem Bildschirm erscheint das Fenster Einstellungen der Richtlinie für **Kaspersky Anti-Virus 5.0 for Windows Workstations**, das mehrere Registerkarten hat.

Die Registerkarten **Allgemein**, **Zusätzliches** und **Bearbeitung von Ereignissen** entsprechen dem Standard für die Anwendung Kaspersky Administration Kit 5.0 (Details s. Hilfesystem für Kaspersky Administration Kit 5.0).

Andere Registerkarten enthalten spezielle Einstellungen für Kaspersky Anti-Virus 5.0 for Windows Workstations. Unten folgt eine detaillierte Beschreibung jeder Registerkarte.

Die Richtlinienparameter für die einzelnen Echtzeitschutz-Komponenten werden nur für jene Computer übernommen, auf denen diese Komponenten installiert sind.

6.2.2.1. Anzeige von Informationen zur Richtlinie

Auf der Registerkarte **Allgemein** (s. Abbildung 69) stehen allgemeine Angaben über die Richtlinie:

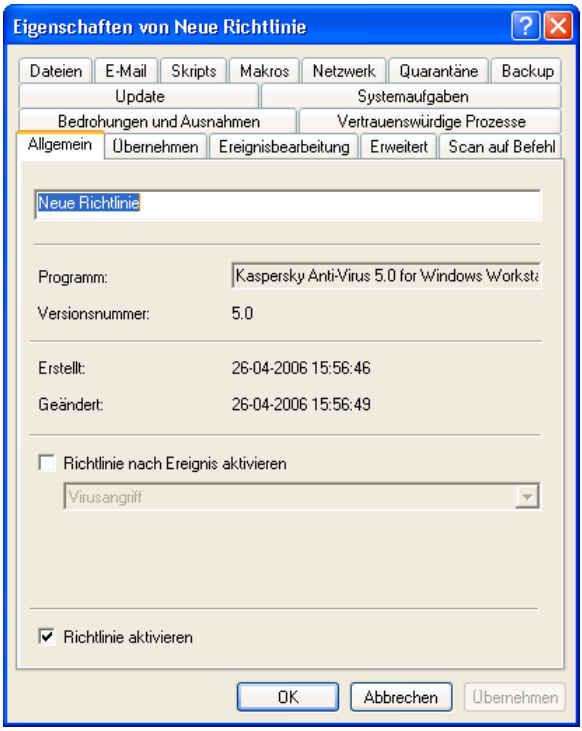

Abbildung 69. Registerkarte **Allgemein**

- Name der Richtlinie*;*
- Anwendung, für die Richtlinie angelegt wurde (**Kaspersky Anti-Virus 5.0 for Windows Workstations**);
- Version der Anwendung;
- Datum und Uhrzeit für die Erstellung der Richtlinie;

- Datum und Uhrzeit für die letzte Änderung der Richtlinie.

Auf dieser Registerkarte können Sie den Namen der Richtlinie ändern.

Wenn Sie möchten, dass einen Richtlinie aktiv wird, setzen Sie das Kontrollkästchen **Richtlinie aktivieren**. Möchten Sie, dass eine Richtlinie beim Eintritt eines bestimmten Ereignisses automatisch aktiviert wird, dann setzen Sie das Kontrollkästchen **Richtlinie nach Ereignis aktivieren** und wählen Sie das gewünschte Ereignis aus der Dropdown-Liste. Die Rückkehr zur vorigen Richtlinie erfolgt manuell.

6.2.2.2. Scan auf Befehl

Auf der Registerkarte **Scan auf Befehl** (s. Abbildung 70) können Sie die Richtlinien-Optionen für den Scan auf Befehl einstellen.

Wählen Sie im Abschnitt Gewählte Schutzstufe aus der Dropdown-Liste eine der drei vordefinierten Stufen für die Antivirensicherheit aus (s. Pkt. 4.2 auf S. 41).

Im Abschnitt **Aktionen für gefundene Objekte** wird der Typ der Aktion festgelegt, die beim Fund infizierter oder verdächtiger Objekte ausgeführt werden soll (Details über die Typen der Aktionen, die von Kaspersky Anti-Virus im Modus 'Scan auf Befehl' ausgeführt werden können, s. Pkt. 5.3.3.2 auf S. 88).

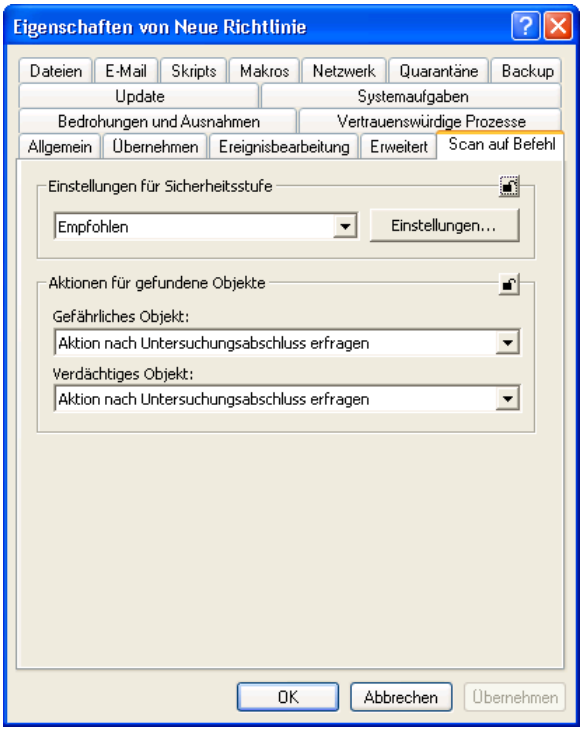

Abbildung 70. Registerkarte **Scan auf Befehl**

Wählen Sie aus der sich öffnenden Liste **Sicherheitsstufe** eine der drei voreingestellten Antiviren-Sicherheitsstufen aus: **Maximaler Schutz**, **Empfohlen**, **Maximales Tempo** (Näheres siehe Punkt 4.2 auf S. 41).

Mit einem Mausklick auf **Details** öffnet sich ein Dialogfeld, in dem Sie zusätzliche Einstellungen der entsprechenden Sicherheitsstufe einsehen oder eigene Einstellungen vornehmen können. Dabei ändert sich die Sicherheitsstufe in **Benutzereinstellungen**.

Das Dialogfeld für genaue Anpassung enthält Registerkarten **Untersuchungsobjekte**, **Aktionen** und **Zusätzlich**.

Auf der Registerkarte **Untersuchungsobjekte** (s. Abbildung 71) können Sie Untersuchungsobjekte auswählen, ihre Art bestimmen (Näheres s. Pkt. 5.3 auf S. 76) und die Ausnahmeliste für die Untersuchung einstellen.

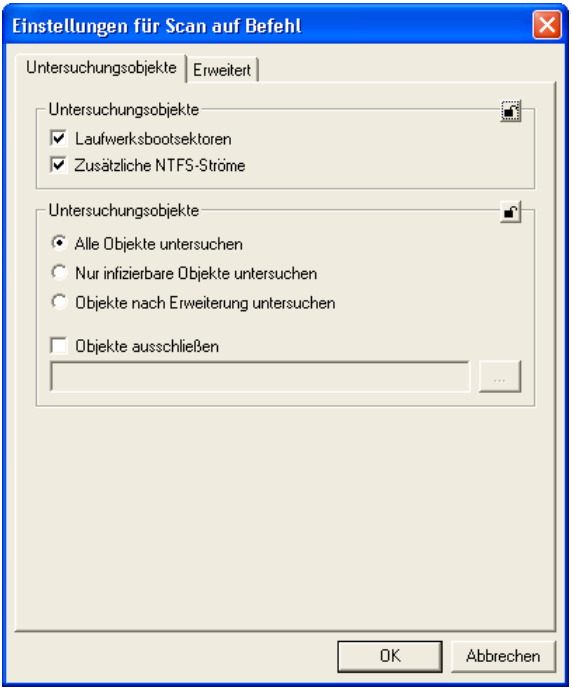

Abbildung 71. Registerkarte **Untersuchungsbereich**

Auf der Registerkarte **Erweitert** (s. Abbildung 72) können Sie die Untersuchung für verschiedene Typen von Compound-Dateien aktivieren/deaktivieren, erlaubte potentiell gefährliche Programme von der Untersuchung ausschließen, Konditionen für die Kennwortabfrage bei der Untersuchung von kennwortgeschützten Archiven sowie einige Einschränkungen für den Untersuchungsvorgang festlegen (Näheres siehe Pkt. 5.3 auf S. 76)..

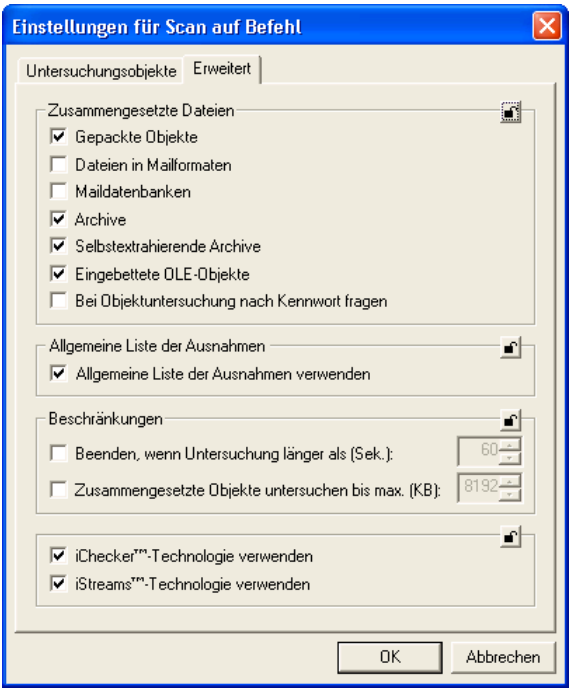

Abbildung 72. Registerkarte **Erweitert**

6.2.2.3. Echtzeitschutz der Objekte des Dateisystems

Die Richtlinienparameter für den Echtzeitschutz für Dateien werden nur für jene Computer übernommen, auf denen diese Komponente installiert ist.

Auf der Registerkarte **Dateien** (s. Abbildung 73) können Sie die Richtlinien-Optionen für den Modus Echtzeitschutz der Objekte des Dateisystems einstellen. Die Auswahl der Sicherheitsstufe und der Wechsel zum Dialogfeld mit den genauen Anpassungen erfolgt wie in der Registerkarte **Benutzerdefinierte Untersuchung** (s. Pkt. 6.2.2.2 auf S. 144).

Im Abschnitt **Aktionen für gefundene Objekte** wird der Typ der Aktion festgelegt, die beim Fund infizierter oder verdächtiger Objekte ausgeführt werden soll (Details über die Typen der Aktionen, die von Kaspersky Anti-Virus im Echtzeitschutzmodus ausgeführt werden können, s. Pkt. 5.2.1.2 auf S. 62).

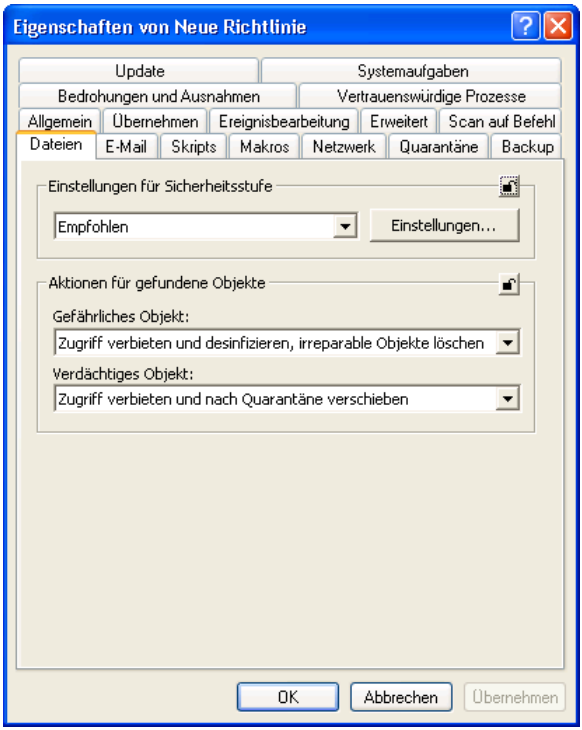

Abbildung 73. Registerkarte **Dateien**

Auf der Registerkarte **Untersuchungsobjekte** (s. Abbildung 74) können Sie die Untersuchungsobjekte festlegen und die Liste mit Ausnahmefällen bearbeiten. Diese Einstellungen gleichen den lokalen Einstellungen, die in Punkt 5.2.1 auf S. 59 beschrieben sind.

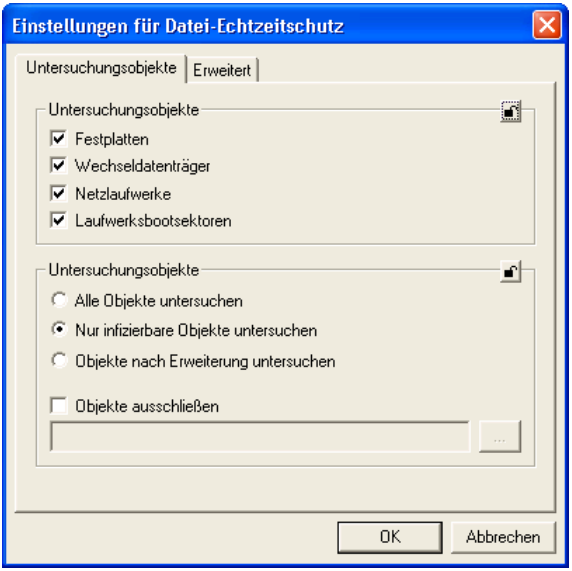

Abbildung 74. Registerkarte **Untersuchungsobjekte**

Auf der Registerkarte **Erweitert** (s. Abbildung 75) können Sie die Untersuchung für verschiedene Typen von zusammen gesetzten Dateien aktivieren/deaktiviere, erlaubte potentiell gefährliche Programme von der Untersuchung ausschließen, Einschränkungen für die Untersuchung einstellen und den Einsatz von iChecker und iStreams zulassen/unterdrücken (Näheres siehe Pkt. 5.2.1 auf S. 59).

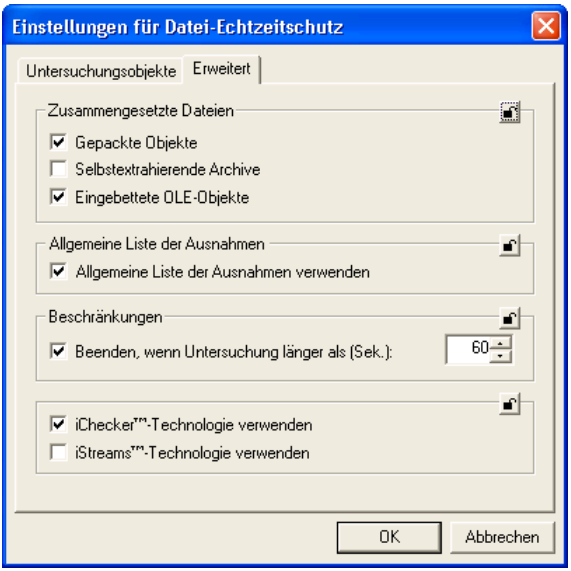

Abbildung 75. Registerkarte **Erweitert**

6.2.2.4. Bedrohungen und Ausnahmen

Auf der Registerkarte **Bedrohungen und Ausnahmen** (s. Abbildung 76) werden die Antiviren-Datenbanken festgelegt, die bei der Untersuchung verwendet werden sollen (standardmäßige oder erweiterte). Außerdem wird hier die Liste der Untersuchungsausnahmen angelegt. Diese Einstellungen entsprechen denen der lokalen Benutzeroberfläche (Details s. Pkt. 5.1.3.5 auf S. 55 und Pkt. 5.7 auf S. 102).

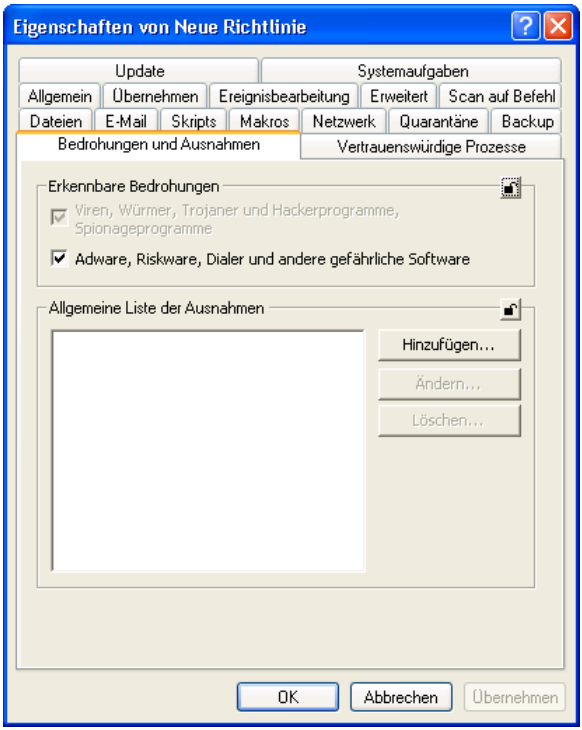

Abbildung 76. Registerkarte **Bedrohungen und Ausnahmen**

6.2.2.5. Aktivitätskontrolle der Programmprozesse

Auf der Registerkarte **Vertrauenswürdige Prozesse** (s. Abb. 77) können Sie die Richtlinieneinstellungen vornehmen, welche die Antivirenkontrolle der Dateiaktivität von Prozessen bestimmter Programme betreffen. Diese Einstellungen entsprechen den Einstellungen des lokalen Interface (Details s. Pkt. 5.5 auf S. 99).

Zur Angabe des Dateipfads muss der Pfad der Prozessdatei auf dem entfernten Computer genannt werden.

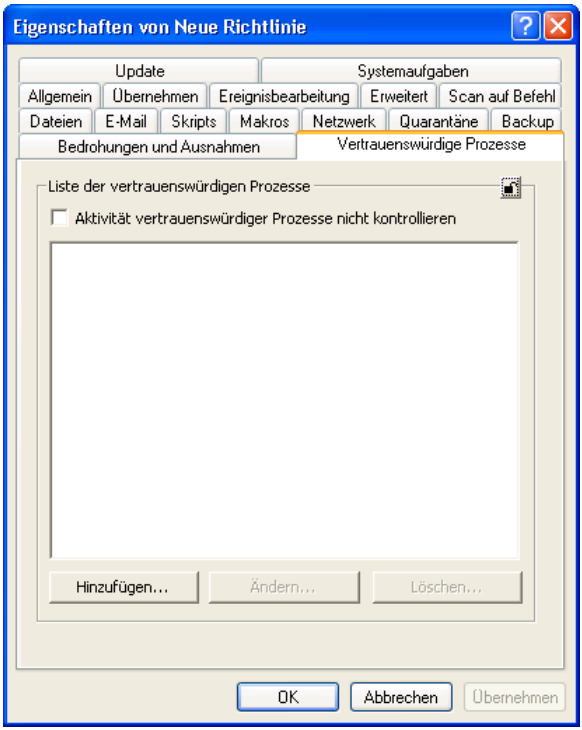

Abbildung 77. Registerkarte **Vertrauenswürdige Prozesse**

6.2.2.6. Untersuchung von E-Mail-Nachrichten

Die Richtlinienparameter für den E-Mail-Echtzeitschutz werden nur für jene Computer übernommen, auf denen diese Komponente installiert ist.

Auf der Registerkarte **E-Mail** (s. Abbildung 78) werden die Richtlinien-Optionen für die Untersuchung der ein- und ausgehenden Nachrichten eingestellt. Die Auswahl der Sicherheitsstufe und der Wechsel in das Fenster zur detaillierten Konfiguration entsprechen der Registerkarte **Scan auf Befehl** (s. Pkt. 6.2.2.2 auf S. 144).

Im Abschnitt **Aktionen für gefundene Objekte** wird der Typ der Aktion festgelegt, die beim Fund infizierter oder verdächtiger Objekte ausgeführt werden soll (Details über die Typen der Aktionen, die von Kaspersky Anti-Virus im Modus für die E-Mail-Untersuchung ausgeführt werden können, s. Pkt. 5.2.2.2 auf S. 68).

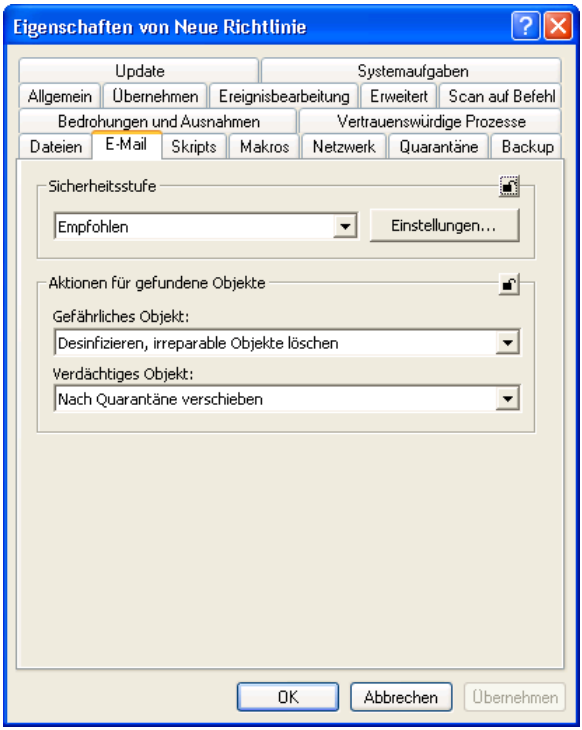

Abbildung 78. Registerkarte **E-Mail**

In der Registerkarte **Untersuchungsobjekte** (s. Abbildung 79) sind die zu untersuchenden Objekte zu wählen bzw. Ausschlüsse aus der E-Mail-Untersuchung einzustellen. Alle Einstellungen gleichen den lokalen Einstellungen. Näheres finden Sie dazu in Punkt 5.2.2 auf S. 64).

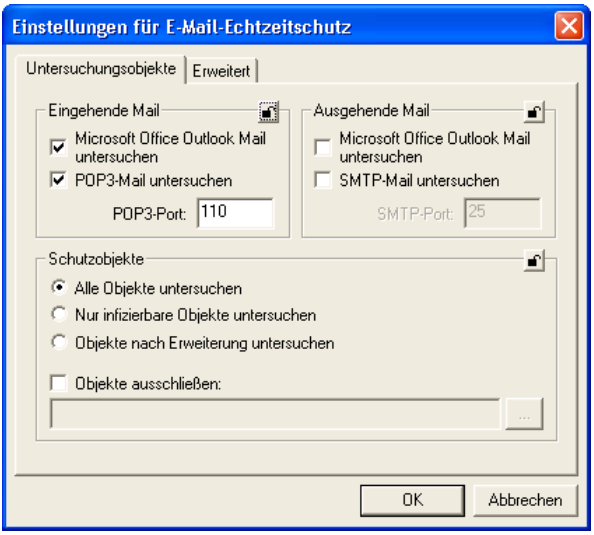

Abbildung 79. Registerkarte **Untersuchungsobjekte**

In der Registerkarte **Erweitert** (s. Abbildung 80) können Sie die Anwendung der iChecker-Technologie zulassen/unterdrücken bzw. einige Untersuchungs-Einschränkungen für E-Mails definieren (Näheres siehe Pkt. 5.2.2 auf S. 64)

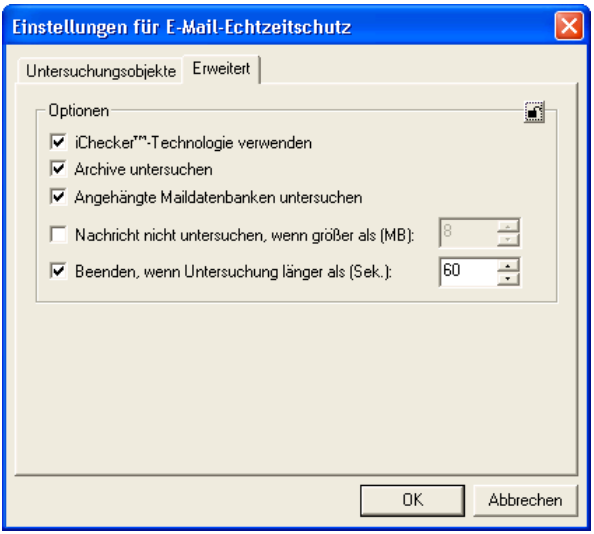

Abbildung 80. Registerkarte **Erweitert**

6.2.2.7. Untersuchung von Skripten

Die Richtlinienparameter für die Skriptuntersuchung werden nur für jene Computer übernommen, auf denen diese Komponente installiert ist.

In der Registerkarte **Skripte** (s. Abbildung 81) können Sie Richtlinien für den Echtzeitschutz gegen potentiell gefährliche Skripte von VBScript und JavaScript einstellen. Wählen Sie eine der folgenden Varianten:

- **Scriptführung blockieren** (gilt als Standardaktion)
- **Ausführung erlauben**
- **Benutzer nach Aktion fragen**

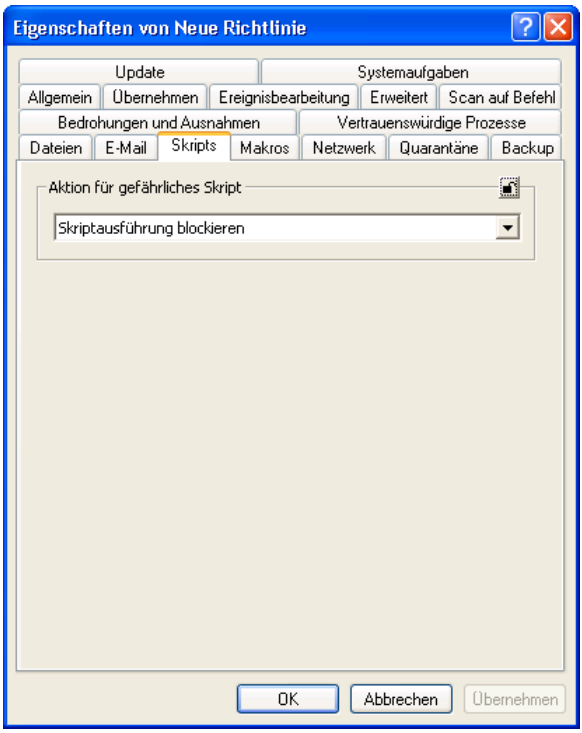

Abbildung 81. Registerkarte **Skripte**

6.2.2.8. Untersuchung von Makros

Die Richtlinienparameter für die Makrountersuchung werden nur für jene Computer übernommen, auf denen diese Komponente installiert ist.

In der Registerkarte **Makros** (s. Abbildung 82) können Sie die Richtlinien für Untersuchung der von MS-Office-Anwendungen genutzten VBA-Makros einstellen.

Die Auswahl der Sicherheitsstufe und der Wechsel zum Dialogfeld mit den genauen Anpassungen erfolgt wie in der Registerkarte **Scan auf Befehl** (s. Pkt. 6.2.2.2 auf S. 144).

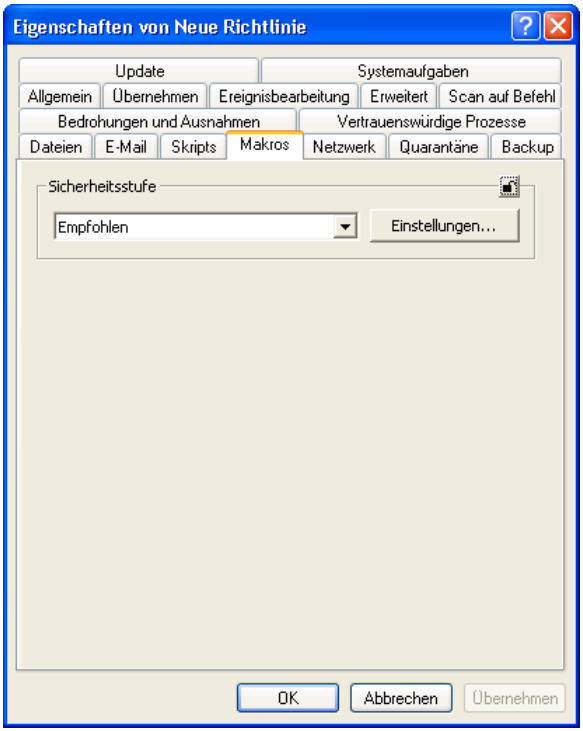

Abbildung 82. Registerkarte **Makros**

Mit einem Mausklick auf **Einstellungen...** (s. Abbildung 82) öffnet sich ein Dialogfeld, in dessen Registerkarten die Hauptarten der vom Kaspersky Anti-Virus kontrollierten Makrobefehle aufgelistet sind.

Standardmäßig sind hier fünf Arten von Makrobefehlen definiert, denen entsprechende Registerkarten zugeordnet sind:

- **Module** – Makrobefehle zur Arbeit mit Projektmodulen:
    - Module kopieren (OrganizerCopy);
    - Module löschen (OrganizerDelete);
    - Module umbenennen (OrganizerRename);
    - Module hinzufügen;
    - Modul löschen;
    - Module importieren;
    - Module exportieren.
- **Zeilen** – Makrobefehle zur Änderung des Makrocode:
    - Anlage einer Prozedur
    - in Modul aus einer Datei Makrozeilen einfügen;
    - zum Makros Zeilen hinzufügen;
    - in Makros Zeilen einfügen;
    - in Makros Zeilen ersetzen;
    - Makrozeilen löschen.
- **Dateien** – Aktionen mit Dateien:
    - Datei löschen;
    - Dateiattribute ändern;
    - Ordner anlegen;
    - Ordner löschen;
    - Datei im Schreibmodus öffnen.
- **ActiveX** – Aktionen mit ActiveX-Objekten:
    - ActiveX-Objekt erstellen;
    - auf einem Fernrechner ein ActiveX-Objekt erstellen;
    - Zugriff auf ActiveX-Objekt.
- **Weiteres** – sonstige Makrobefehle:
    - Anfrage für Speichern der Vorlage Normal.dot deaktivieren;

- Excel-Arbeitsblätter kopieren;
- Virenschutz abschalten;
- Ausführung des MacroCopy-Befehls;
- Ausführung des Shell-Befehls;
- API-Funktion aufrufen;
- Tastatureingaben simulieren.

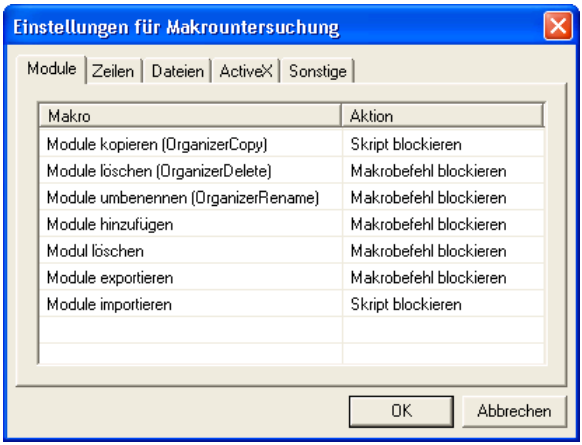

Abbildung 83. Auflistung der Makros

Neben jedem Makrobefehl wird in der Spalte **Aktion** (s. Abbildung 83) je nach der gewählten Sicherheitsstufe ein Aktionstyp definiert, der vom Anti-Virus beim Erkennen von diesem Makrobefehl ausgeführt wird. Es gibt folgende Möglichkeiten:

- *Makrobefehl zulassen,*
- *Nach Action fragen,*
- *Makrobefehl unterdrücken,*
- *Skript unterdrücken* – Abbrechen der Makroaktion.

Um die vom Kaspersky Anti-Virus beim Erkennen eines verdächtigen Makrobefehls auszuführende Aktion zu ändern,

klicken Sie den neben dem betreffenden Makrobefehl angegebenen Aktionsnamen mit der linken Maustaste an und wählen Sie aus der sich öffnenden Liste eine andere Aktion aus.

6.2.2.9. Schutz vor Netzwerkangriffen

Die Richtlinienparameter für den Schutz vor Netzwerkangriffen werden nur für jene Computer übernommen, auf denen diese Komponente installiert ist.

Auf der Registerkarte **Netzwerk** (s. Abbildung 84) können Sie die Parameter für den Schutz vor Netzwerkangriffen anpassen. Die Einstellungen entsprechen denen der lokalen Oberfläche (Details s. Pkt. 5.2.6 auf S. 74).

Geben Sie im Abschnitt **Aktion bei erforderlichem Neustart** die Aktion an, die beim Download eines Updates für die Angriffsdatenbank sowie beim Aktivieren/Deaktivieren des Schutzes vor Netzwerkangriffen ausgeführt werden soll (s. Pkt. 5.2.6 auf S. 74). Wählen Sie eine der folgenden Varianten:

- *Benutzer fragen*. In diesem Fall erscheint auf dem Bildschirm ein Fenster mit einer Anfrage zum Neustart der Workstation.
- *Benutzer nicht fragen und bis zum nächsten Neustart des Computers aufschieben*. Diese Aktion gilt als Standard.
- *Sofort neu starten*. In diesem Fall wird die Workstation sofort nach dem Download eines Updates für die Datenbanken der Netzwerk-Angriffe neu gestartet.

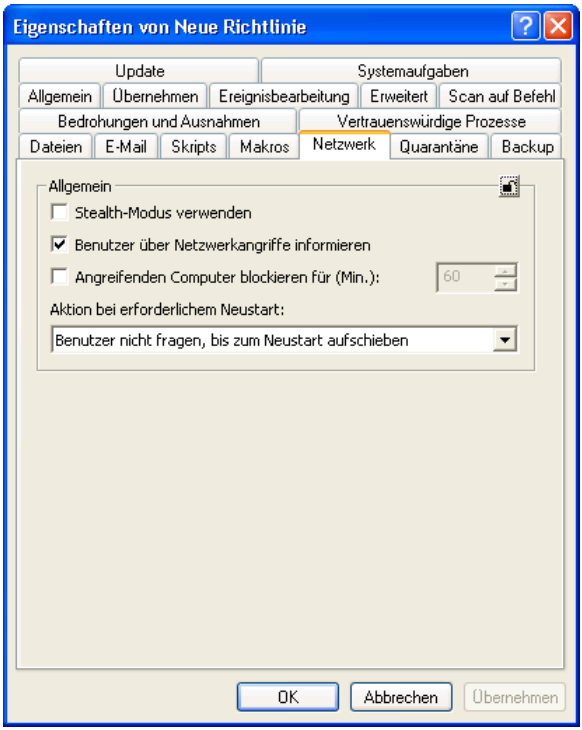

Abbildung 84. Registerkarte **Netzwerk**

6.2.2.10. Update der Antiviren-Datenbanken und Anwendungsmodule

In der Registerkarte **Update** (s. Abbildung 85) können Sie die Einstellungen für den Update-Service für Antiviren-Datenbanken und Anwendungsmodule ändern, die Sie bei Erstellung der Richtlinie vorgenommen haben.

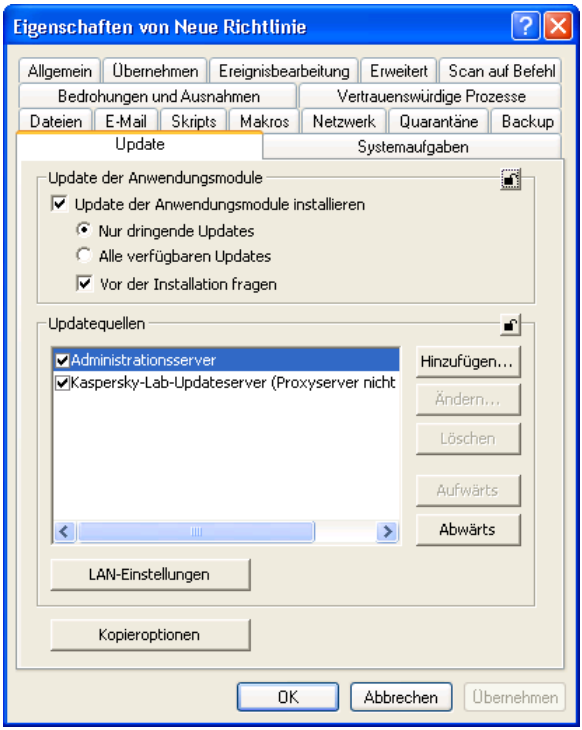

Abbildung 85. Registerkarte **Update**

Die Registerkarte **Update** besteht aus folgenden Bereichen: **Update der Anwendungmodule installieren** – hier können die Parameter für Update-Service für Antiviren-Datenbanken eingestellt werden: (s. Schritt 5. auf S. 140), **Update-Quelle** – Angabe und Einstellung der Update-Quelle für die Antiviren-Datenbanken und die Anwendungsmodule (s. Schritt 3 auf S. 139).

Mit Hilfe der Schaltfläche **LAN-Einstellungen** können Sie den Proxyserver anpassen (Details s. Pkt. 5.1.3.4 auf S. 53). Im folgenden Fenster können Sie im Feld **Zeitlimit für Verbindung (Sek.)** die Wartezeit für die Verbindung mit dem Updateserver (in Sekunden) festlegen. Bei einer Überschreitung der vorgegebenen Wartezeit wechselt die Aufgabe zu einer anderen Updatequelle (aus der Liste) oder das Update wird abgebrochen (wenn keine andere Updatequelle angegeben wurde).

Im Fenster, das durch Klick auf die Schaltfläche **Kopieroptionen** geöffnet wird, können Sie ein Kopieren von Updates in ein lokales Verzeichnis aktivieren und deren Optionen einstellen (s. Pkt. 5.1.3 auf S. 46).

6.2.2.11. Aktionen mit den Systemaufgaben

Auf der Registerkarte **Systemaufgaben** (s. Abbildung 86) können Sie den automatischen Start von Systemaufgaben, die nach Zeitplan gestartet werden, und von Echtzeitschutz-Aufgaben auf Remote-Workstations, die zu einer Administrierungsgruppe gehören, aktivieren/deaktivieren.

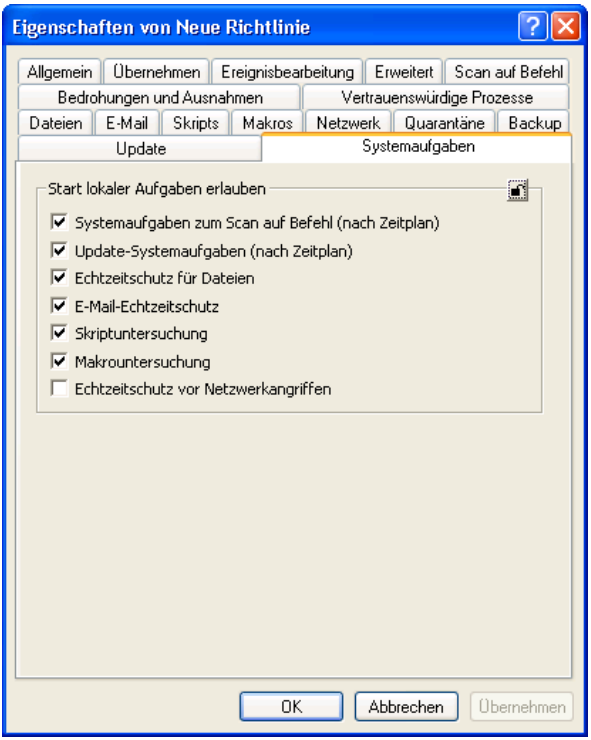

Abbildung 86. Registerkarte **Systemaufgaben**

6.2.2.12. Einstellungen der Quarantäne und Backup

In den Registerkarten **Quarantäne** (s. Abbildung 87) und **Backup** (s. Abbildung 88) können Sie die Richtlinie für diese Ablagen einstellen.

Diese Einstellungen entsprechen den Einstellungen der Quarantäne und des Backups bei Verwaltung über eine lokale Schnittstelle (s. Pkt. 5.10.1 auf S. 112).

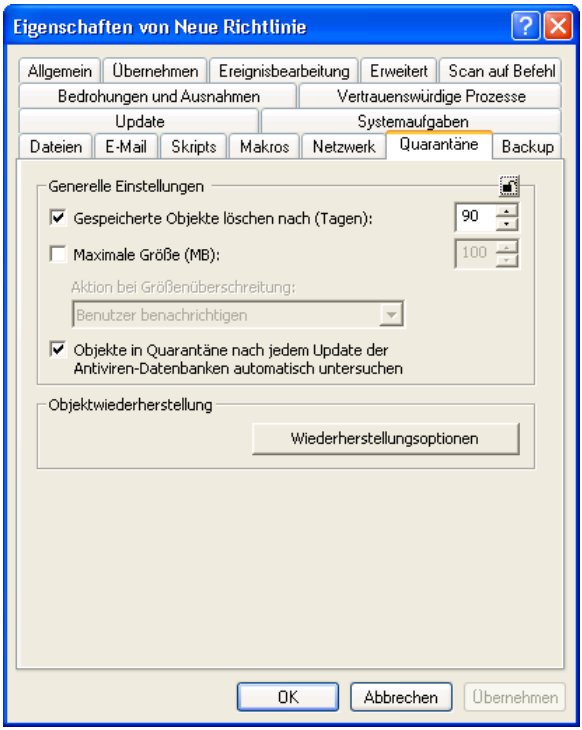

Abbildung 87. Registerkarte **Quarantäne**

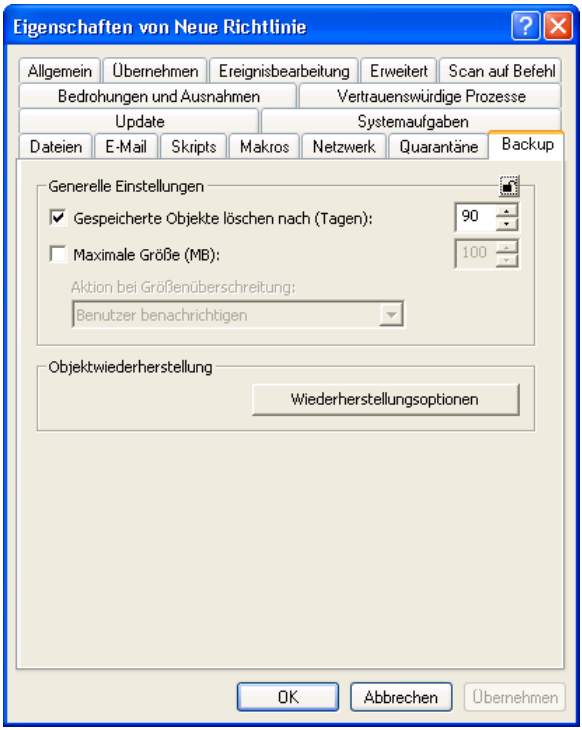

Abbildung 88. Registerkarte **Backup**

6.2.2.13. Schaffung des Protokolls über die Arbeit der Anwendung

Auf der Registerkarte **Ereignisbearbeitung** (s. Abbildung 89) stehen die Ereignistypen, die bei der Arbeit des Programms eintreten und im Protokoll festgehalten werden sowie der Speicherort des Protokolls und der Modus für die Benachrichtigung des Systemadministrators und / oder anderer Benutzer.

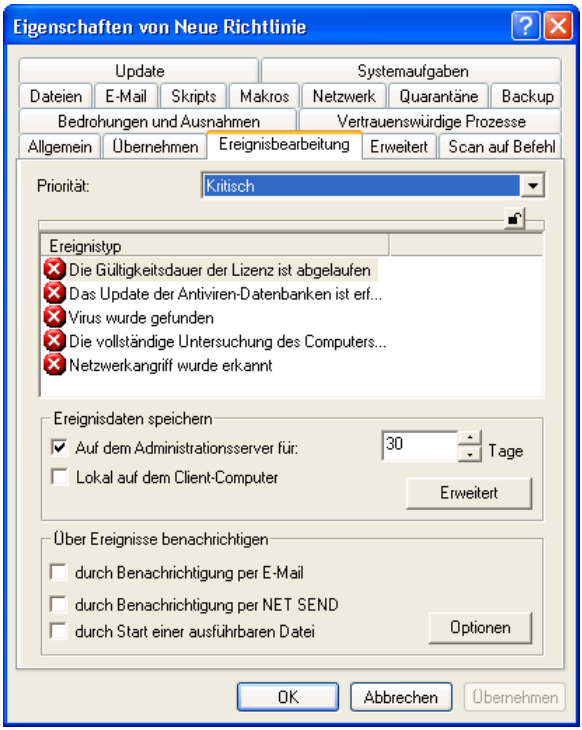

Abbildung 89. Registerkarte **Ereignisbearbeitung**

Während des Betriebs generiert Kaspersky Anti-Virus 5.0 for Windows Workstations einen bestimmten Satz von Ereignissen (s. Tabelle 2). Jedes Ereignis verfügt über eine Charakteristik, die dessen Wichtigkeitsstufe beschreibt. Es gibt vier Wichtigkeitsstufen:

- **Kritisch**
- **Fehler**
- **Warnung**
- **Informationen**

Ereignisse eines Typs können unterschiedliche Wichtigkeitsstufen besitzen. Dies hängt von der Situation ab, in der das Ereignis eingetreten ist.

Aus dem Dropdown-Feld **Priorität** wählen Sie die Bedeutungsstufe für die Ereignisse. Im Informationsfeld unter der Liste stehen die Ereignistypen für die ausgewählte Stufe.

Tabelle 2. Ereignisse der Anwendung

Ereignis	Wichtigkeitsstufe
Objekt wurde desinifziert	**Warnung**
Infiziertes Objekt wurde gelöscht	**Warnung**
Sicherheitsstufe für Echtzeitschutz wurde geändert	**Information**
Lizenz läuft ab (zwei Wochen zum Ablauf)	**Warnung**
Lizenz abgelaufen	**Kritisch**
Lizenz hat Überprüfung nicht bestanden	**Fehler**
Verdächtiges Objekt gefunden	**Warnung**
Funktionsfehler	**Warnung** **Fehler**
Update der Antiviren-Datenbanken wurde nicht ausgeführt: - seit einer Woche* - seit zwei Wochen*	 **Warnung** **Kritisch**
Virus gefunden	**Kritisch**
Netzwerkangriff wurde erkannt	**Kritisch**
Interner Fehler	**Fehler**
System wurde neu gestartet	**Warnung**
Die Anwendung wurde neu gestartet	**Warnung**
Ein kennwortgeschütztes Archiv wurde erkannt	**Warnung**

Ereignis	Wichtigkeitsstufe
Das Objekt wurde nicht gesäubert	**Warnung**
Die vollständige Untersuchung des Computers liegt weit zurück: – vor zwei Wochen* – vor einem Monat*	 **Warnung** **Kritisch**
Infiziertes Objekt wurde blockiert	**Warnung**
Infiziertes Objekt wurde übersprungen	**Warnung**

* Diese Werte werden standardmäßig aktiviert, können aber im Fenster **Benachrichtigungen** (s. Pkt. 6.2.2.13 auf S. 164) geändert werden.

Sie können für jedes Ereignis angeben, ob es in das Protokoll geschrieben werden soll und Sie können einstellen, ob der Systemadministrator bei Eintreten des Ereignisses benachrichtigt werden soll.

Nähere Beschreibung der übrigen Einstellungen in der Registerkarte **Bearbeitung von Ereignissen** siehe Hilfesystem für Kaspersky Administration Kit 5.0.

6.2.2.14. Registerkarte Erweitert

Auf der Registerkarte **Erweitert** (s. Abbildung 90) stehen Einstellungen der Service-Parameter für Kaspersky Anti-Virus 5.0 for Windows Workstation. Die Mehrzahl der Einstellungen gleicht den Zusatzoptionen, die in Punkt 5.10.4 auf S. 125 beschrieben sind.

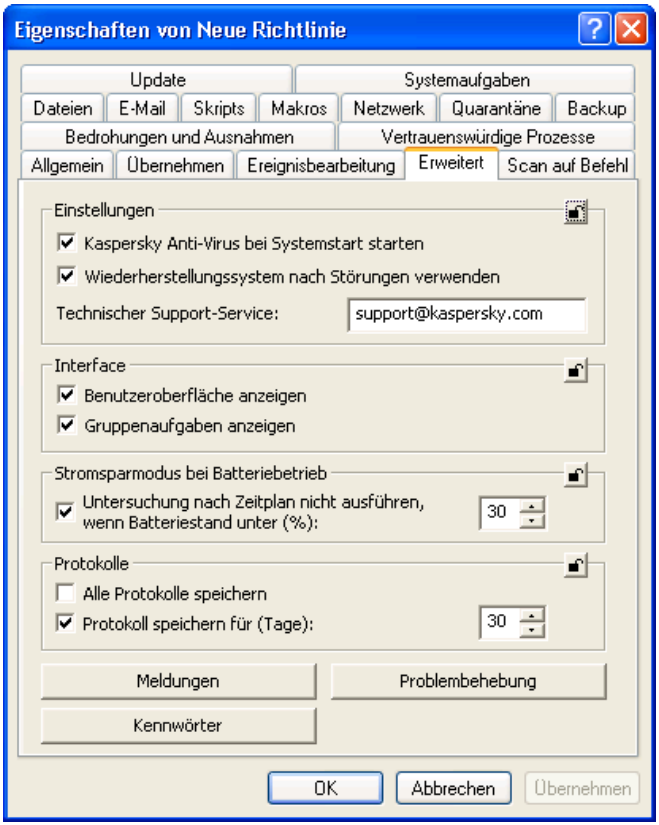

Abbildung 90. Registerkarte **Erweitert**

In dem Fenster, das sich mit einem Klick auf die Schaltfläche **Kennwort für Deinstallation** (s. Abbildung 91) öffnet, können folgende Kennwörter festgelegt werden:

- Kennwort zum Umschalten vom Benutzermodus in den Administratormodus (s. Pkt. 5.10.7 auf S. 131). Um diesen Modus zu aktivieren, setzen Sie das Kontrollkästchen **Kennwort zum Programmschutz verwenden**.
- Kennwort, das erfragt wird, wenn Kaspersky Anti-Virus deinstalliert werden soll. Dadurch lässt sich die unerlaubte Deinstallation von Kaspersky Anti-Virus von einer Workstation verhindern.

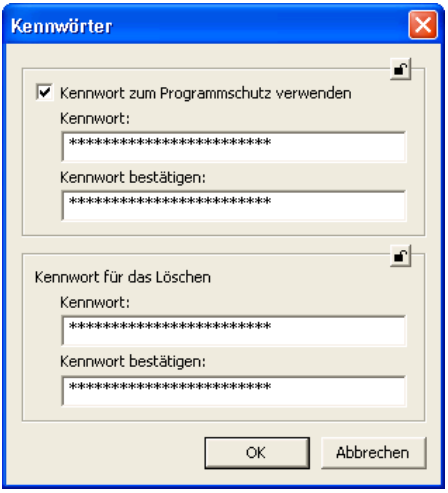

Abbildung 91. Fenster **Kennwörter**

Im Fenster (s. Abbildung 92), das sich mit dem Klick auf die Schaltfläche **Einstellungen für Bestätigungen** öffnet, können Sie die Konfigurationen für den Empfang der verschiedenen Benachrichtigungen einstellen.

- **Bestätigungsanfrage beim Abbrechen der Untersuchung –** dem Benutzer die Anzeige der Meldungen, die über erkannten Viren informieren, zur Verfügung zu stehen.
- **Bestätigungsanfrage beim Laden/Ausladen des Programms** – Auf dem Bildschirm dürfen Meldungen angezeigt werden, welche die Arbeit von Kaspersky Anti-Virus begleiten.
- **Bestätigungsanfrage beim Deaktivieren des Echtzeitschutzes** – Das animierte Symbol von Kaspersky Anti-Virus darf in der Taskleiste angezeigt werden, wenn eine Virensuche stattfindet.
- **Bestätigungsanfrage zur Bearbeitung gefährlicher Objecte**– Die während der Arbeit von Kaspersky Anti-Virus auf dem Bildschirm angezeigten Meldungen werden von Tonsignalen begleitet.

Im Abschnitt **Benachrichtigungen über Ereignisse** können Sie die Konfigurationen für den Empfang der Benachrichtigungen über den Zustand der Aktualisierungsaufgaben von Antiviren-Datenbanken und vollständiger Untersuchung des Rechners. Für jede dieser Aufgaben sind zwei Stufen von Ereignissen vorgesehen – **Warnung** und **Kritisches Ereignis**.

Im rechts befindlichen Feld bestimmen Sie den Zeitraum in Tagen, nach denen der Benutzer beim Starten von Kaspersky Anti-Virus täglich die entsprechende Benachrichtigung empfangen wird. Dieser Zeitraum zählt ab Datum der letzten Ausführung der entsprechenden Aufgabe.

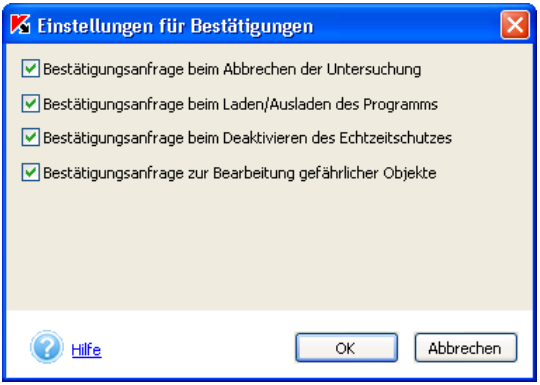

Abbildung 92. Fenster **Einstellungen für Bestätigungen**

Im Fenster (s. Abbildung 93), das mit der Schaltfläche **Problembehebung** geöffnet wird (s. Abbildung 90), erfolgen Einstellungen, die dazu dienen, die Ausführung von Aufgaben zum Scan auf Befehl zu optimieren. Sie können:

- **Mailuntersuchung bei Aufgabenausführung deaktivieren** – Deaktivieren der E-Mail-Untersuchung während der Ausführung einer Aufgabe zur Untersuchung des Arbeitsplatzes.
- **Antivirenuntersuchung anhalten bei Systemauslastung über (%)** – Anhalten einer auf Befehl gestarteten Antivirenuntersuchung, wenn die Auslastung des Dateisystems über das festgelegte Niveau (in Prozent) steigt. Geben Sie mit Hilfe des Schiebereglers oder im rechts angebrachten Feld den Wert des zulässigen Systemauslastungsniveaus an.

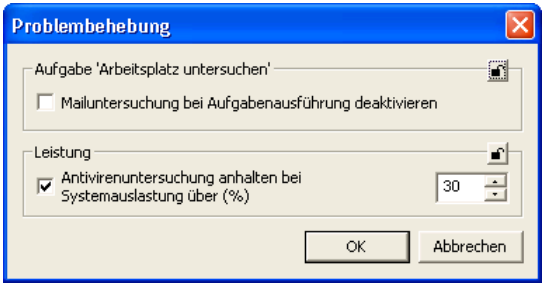

Abbildung 93. Fenster **Problembehebung**

6.2.2.15. Anzeige der Ergebnisse des Übernehmens von der Richtlinie

In der Registerkarte **Übernehmen** (s. Abbildung 94) finden Sie Hilfethemen zur Anwendung der Richtlinie für eine Rechnergruppe. Dabei wird die Anzahl der Rechner angegeben:

- für welche die Richtlinie definiert wurde;
- auf welchen diese ausgeführt wurde;
- auf welchen diese noch nicht ausgeführt wurde;
- auf welchen die Richtlinie wegen eines Fehlers nicht ausgeführt wurde.

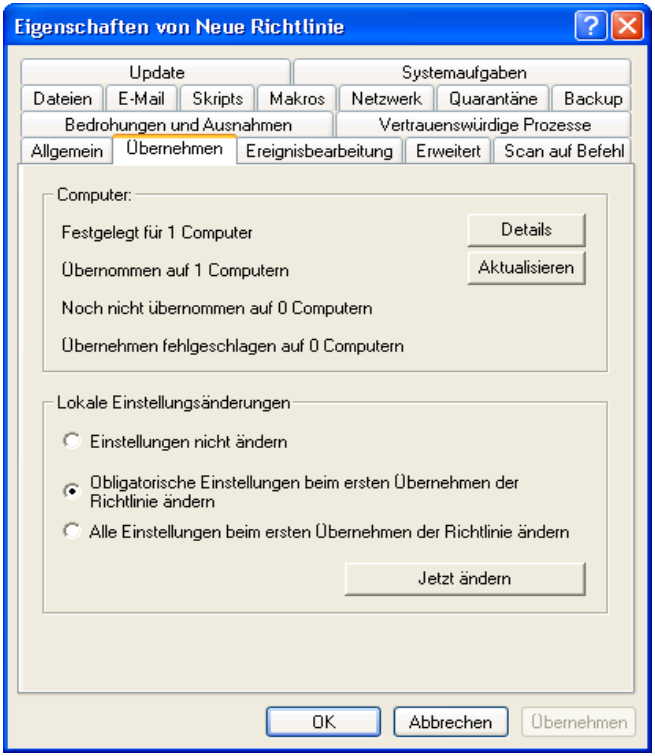

Abbildung 94. Registerkarte **Übernehmen**

Detaillierte Ergebnisse der Richtlinien-Anwendung auf jedem zur Gruppe gehörenden Client können Sie im Dialogfeld einsehen, das über die Schaltfläche

Details aufgerufen wird (Näheres siehe Hilfesystem für Kaspersky Administration Kit 5.0).

Im Abschnitt **Lokale Einstellungsänderungen** können Sie angeben, welche Parameter in den Richtlinien untergeordneter Gruppen, in den Anwendungseinstellungen und in den Aufgabeneinstellungen auf Client-Computern beim ersten Übernehmen der Richtlinie geändert werden sollen. Folgende folgenden Varianten stehen zur Auswahl:

- **Einstellungen nicht ändern.** In diesem Fall werden die lokalen Parameter nicht geändert.
- **Obligatorische Einstellungen beim ersten Übernehmen der Richtlinie ändern**. In diesem Fall werden solche lokalen Parameter geändert, neben denen in den Richtlinieneinstellungen das Symbol steht. Um das Ändern von obligatorischen Parametern auf den Client-Computern durch einen Benutzer zu verbieten, klicken Sie mit der linken Maustaste auf das Symbol. Es ändert sich dadurch in .
- **Alle Einstellungen beim ersten Übernehmen der Richtlinie ändern.** In diesem Fall werden alle lokalen Parameter in Übereinstimmung mit den Richtlinienparametern geändert. Ebenso wie bei der vorhergehenden Variante können Sie ein Verbot für das Ändern von obligatorischen Parametern durch den Benutzer festlegen.

Die Änderung der lokalen Parameter erfolgt automatisch beim ersten Übernehmen der Richtlinie auf dem Client-Computer. Wenn Sie die Richtlinie mit aktualisierten Parametern erneut übernehmen möchten, klicken Sie auf die Schaltfläche **Jetzt ändern**.

6.3. Aufgabenverwaltung

In diesem Abschnitt finden Sie Informationen zur Erstellung und Verwaltung der Aufgaben für Kaspersky Anti-Virus 5.0 for Windows Workstations. Näheres zum Konzept der Aufgabenverwaltung siehe Administratorhandbuch für Kaspersky Administration Kit 5.0.

6.3.1. Aufgabenerstellung

Mit der Anwendungsinstallation wird für jeden Rechner eine Systemaufgabenliste erstellt. In dieser Liste (s. Abbildung 95) stehen Aufgaben des Echtzeitschutzes (Schutz für Dateien, E-Mail, Untersuchung von Makros und Skripten), Untersuchungsaufgaben (Untersuchung von Mein Computer, Automatische Untersuchung beim Start von Kaspersky Anti-Virus, Untersuchung der Quarantäne) und Update-Aufgaben (Aktualisierung der Antiviren-

Datenbanken, Aktualisierung der Programmmodule, Rückgängigmachen der Datenbank-Updates).

Aufgaben des Echtzeitschutzes sind einmalig und werden im Hintergrund ausgeführt. Es wurde einen Zeitplan für Untersuchungsaufgaben und Update-Aufgaben von Antiviren-Datenbanken erstellt.

Sie können Systemaufgaben standardmäßig starten, deren Optionen und Zeitplan einstellen; diese Aufgaben können nicht gelöscht werden.

Bei der Verwaltung des Kaspersky Anti-Virus über Kaspersky Administration Kit 5.0 können Sie folgende Aufgaben erstellen:

- lokale Aufgaben – diese werden für einzelne Clients definiert;
- Gruppenaufgaben – diese werden für Gruppen von Clients definiert;
- Globale Aufgaben – diese werden für ausgewählte Clients aus beliebigen Gruppen des logischen Netzes definiert.

Sie können Aufgabeneinstellungen ändern, Aufgabenerfüllung verfolgen, mit Hilfe von Standardbefehlen **Kopieren/Einfügen**, **Ausschneiden/Einfügen** und **Löschen** im Kontextmenü bzw. ähnlicher Befehle im Menü **Aktion** Aufgaben kopieren bzw. von einer Gruppe auf eine andere übertragen oder löschen.

Die Optionen für den Programmbetrieb auf jedem einzelnen Client werden gemäß Gruppenrichtlinie, Aufgabeneinstellungen und Einstellungen dieser Anwendung auf dem jeweiligen Client bestimmt.

Die Aufgaben werden gemäß ihrem Zeitplan gestartet. Sie können die Aufgaben aus der Liste nach Zeitplan gestarteten Aufgaben vorübergehend ausschließen. Dabei werden die Aufgaben nicht gelöscht, werden aber nicht gestartet.

Sie können eine Aufgabe starten, abbrechen, anhalten oder deren Ausführung wieder aufnehmen. Dies erfolgt manuell aus dem Kontextmenü mit den Befehlen **Start/Stopp/Pause/Weiter** bzw. mit Hilfe gleicher Punkte aus dem Menü **Aktion**.

6.3.1.1. Erstellung lokaler Aufgaben

Um eine lokale Aufgabe zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Gruppen** den Ordner mit dem Namen der Gruppe, zu welcher der betreffende Client gehört.
2. Wählen Sie aus der Ergebnisleiste den Rechner aus, für welchen die lokale Aufgabe zu erstellen ist, und benutzen Sie den

Kontextmenü-Befehl **Eigenschaften** oder den gleichen Punkt im Menü **Aktion**. Danach erscheint im Programmhauptfenster das Dialogfeld **Eigenschaften von <Computername>**, in dem Sie die Eigenschaften des jeweiligen Rechners einsehen können (s. Abbildung 95).

3. Wechseln Sie in die Registerkarte **Tasks** (s. Abbildung 95). In dieser Registerkarte finden Sie die vollständige Auflistung von den für den betreffenden Client erstellten Aufgaben.
   Die Erstellung einer neuen Aufgabe erfolgt über die Schaltfläche **Hinzufügen**. Um eine Aufgabe anzupassen, klicken Sie auf **Eigenschaften**. Mit der Schaltfläche **Löschen** können Sie die aus der Liste gewählte Aufgabe löschen.

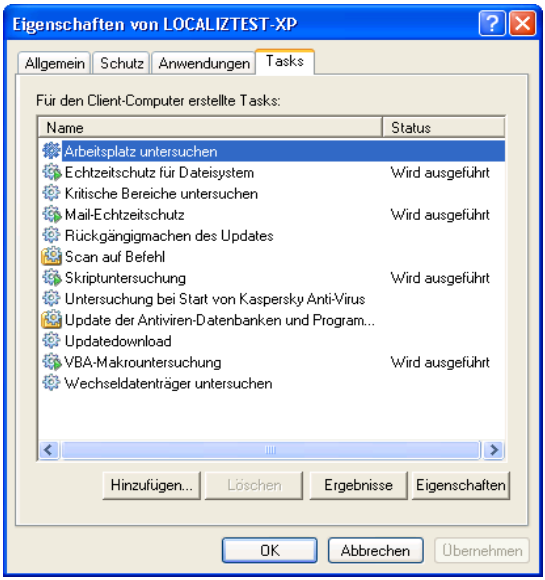

Abbildung 95. Erstellung einer lokalen Tasks
Registerkarte **Tasks**

Beim Anklicken der Schaltfläche **Hinzufügen** erscheint ein Fenster, in dem Sie eine neue Aufgabe erstellen können. Die Benutzeroberfläche ist ähnlich wie ein Microsoft Windows-Assistent (Windows Wizard) gestaltet und besteht aus einer Abfolge von Fenstern (Schritten), zwischen denen mit Hilfe von Schaltflächen **Zurück** und **Weiter** gewechselt werden kann. Um den Assistenten zu beenden, klicken Sie auf **Fertig stellen**. Das Programm kann an jedem beliebigen Punkt durch einen Klick auf **Abbrechen** beendet werden.

Schritt 1. Eingabe allgemeiner Daten zur Aufgabe

Das erste Dialogfelder des Assistenten dient zur Eingabe von Informationen: Hier ist der Name der Aufgabe einzugeben (Feld **Name**).

Schritt 2. Auswahl der Anwendung und des Aufgabentyps

Wählen Sie aus der sich öffnenden Liste **Wählen Sie einen Anwendung aus, für die eine neue Gruppenpolicy erstellt werden soll** die Anwendung **Kaspersky Anti-Virus 5.0 for Windows Workstations.** Der Aufgabentyp wird aus der sich öffnenden Liste **Tasktyp auswählen** gewählt. Für Kaspersky Anti-Virus 5.0 for Windows Workstation können folgende Aufgaben erstellt werden:

- **Update der Antiviren-Datenbanken und der Anwendungsmodule** – Aktualisierung der Antiviren-Datenbanken und der Programmkomponenten.
- **Rückgängigmachen des Updates der Antiviren-Datenbanken** – Updates für Antiviren-Datenbanken rückgängig machen.
- **Scan auf Befehl** – Objekt auf Anfrage untersuchen.
- **Installation des Lizenzschlüssels** – Lizenzschlüssel installieren.

Schritt 3. Einstellung des gewählten Aufgabentyps

Die Inhalte weiterer Dialogfelder unterscheiden sich je nach dem beim vorhergehenden Schritt gewählten Aufgabentyp:

EINSTELLUNGEN FÜR DIE AUFGABE UPDATE

Die Parametereinstellungen in den bei Erstellung der Aufgabe „Antiviren-Datenbanken und Anwendungsmodule aktualisieren“ gleichen den Einstellungen, die während der Erstellung einer Richtlinie vorgenommen werden (s. Schritt 4. –Schritt 5. auf Seiten 139–140). Außerdem können bei Aufgabenerstellung Einstellungen für Kopieren der eingegangenen Updates vorgenommen werden (Näheres s. Pkt. 5.1.3.3 auf S. 51).

EINSTELLUNGEN FÜR DIE AUFGABE ANTIVIREN-DATENBANKEN RÜCKGÄNGIG MACHEN

Die Aufgabe „Updates für Antiviren-Datenbanken rückgängig machen“ hat keine spezifischen Einstellungen. Daher wechseln Sie gleich nach der Auswahl dieses Aufgabentyps in das Dialogfeld mit Zeitplaneinstellungen (s. Pkt. 5.8 auf S. 106).

EINSTELLUNGEN FÜR DIE AUFGABE SCAN AUF BEFEHL

Wählen Sie für die Aufgabe „Objekt auf Befehl untersuchen“ die erforderliche Sicherheitsstufe aus (siehe Punkt 4.2 auf S. 33) und geben Sie die Aktion an, die auf ein gefundenes schädliches Objekt angewandt werden soll (s. Pkt. 5.3.3.2 auf S. 88).

Mit einem Mausklick auf **Detailseinstellung** öffnet sich ein Dialogfeld, in dem Sie zusätzliche Einstellungen der entsprechenden Sicherheitsstufe einsehen oder eigene Einstellungen vornehmen können. Dabei ändert sich die Sicherheitsstufe in **Benutzereinstellungen**.

Im darauf folgenden Dialogfeld (s. Abbildung 96) wählen Sie die zu untersuchenden Objekte mithilfe der Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** aus.

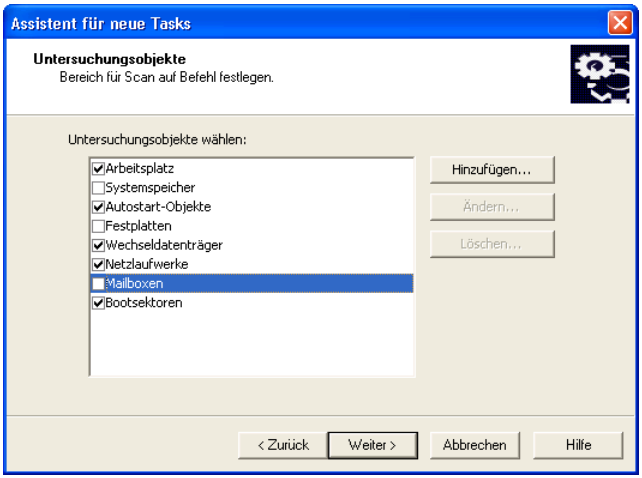

Abbildung 96. Auflistung der zu untersuchenden Objekte

EINSTELLUNGEN FÜR DIE AUFGABE INSTALLATION LIZENZSCHLÜSSEL

Geben Sie für die Aufgabe „Lizenzschlüssel installieren“ den Pfad zur Schlüssel-Datei über die Schaltfläche **Durchsuchen** an. Um den hinzugefügten Schlüssel zu aktivieren, setzen Sie das Häkchen ☑ **Als aktuellen Lizenzschlüssel verwenden**.

Wird ein Schlüssel als Reserveschlüssel hinzugefügt, so ist dieses Optionskästchen nicht zu aktivieren. Mit dem Ablauf des derzeit gültigen Lizenzschlüssels wird der Reserveschlüssel aktiviert.

Schritt 4. Konfiguration des Aufgabenstarts im Namen eines bestimmten Benutzers

Bei diesem Schritt (s. Abbildung 97) können Sie den Start einer erstellten Aufgabe unter dem Namen eines Benutzerkontos konfigurieren, der über ausreichende Zugriffsrechte für ein Untersuchungsobjekt oder für eine Updatequelle verfügt (Details s. Pkt. 5.9 auf S. 110).

Abbildung 97. Konfiguration des Aufgabenstarts unter einem bestimmten Benutzerkonto

Schritt 5. Einstellung des Zeitplans

Nachdem Sie den gewählten Aufgabentyp eingestellt haben, erscheint das Dialogfeld **Einstellungen für den Zeitplan des Task-Starts** (s. Abbildung 98), wo ein Zeitplan festzulegen ist, nach dem diese Aufgabe laufen wird.

Aus der sich öffnenden Liste **Start nach Zeitplan** wählen Sie den benötigten Modus für den Aufgabenstart. Es gibt folgende Möglichkeiten: *Alle n Stunden, Alle n Tage, Alle n Wochen, Manuell, bei Anwendungsstart.* Je nach der gewählten Variante ändert der zentrale Teil des Dialogfeldes mit den Feldern für Dateneingabe seine Ansicht.

Die Aufgabe Rückgängigmachen der Antiviren-Datenbanken und Installation des Lizenzschlüssels kann nur manuell aufgerufen werden.

Näheres zur Anpassung des zeitgesteuerten Autostarts für Aufgaben siehe Hilfesystem für Kaspersky Administration Kit 5.0.

Schritt 6. Fertigstellung der Aufgabenerstellung

Im letzten Dialog informiert Sie der Assistent über die erfolgreiche Fertigstellung der Aufgabenerstellung.

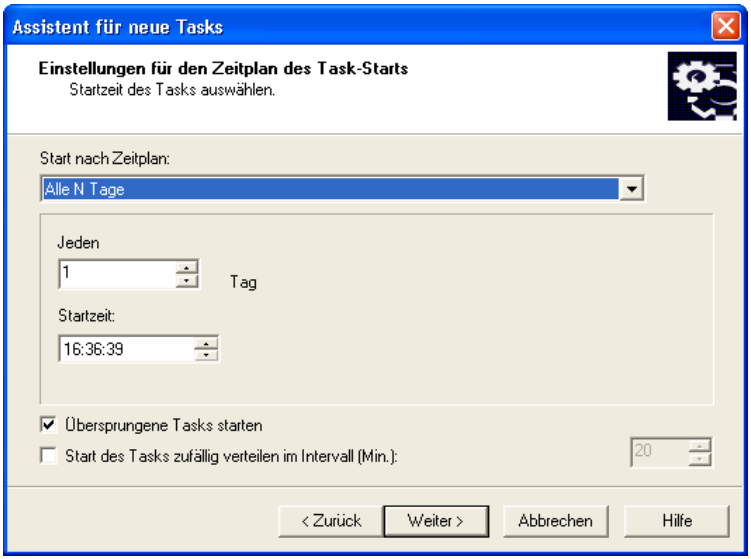

Abbildung 98. Einstellung des Zeitplans bei Aufgabenerstellung

6.3.1.2. Erstellung einer Gruppenaufgabe

Um eine Gruppenaufgabe für Kaspersky Anti-Virus zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Konsoleverzeichnis die Gruppe, für die Sie die Aufgabe erstellen möchten.
2. Wählen Sie den zu dieser Gruppe gehörenden Ordner **Gruppenaufgaben** aus, rufen Sie das Kontextmenü auf und wählen Sie den Befehl **Neu→Task** aus oder benutzen Sie den gleichen Punkt im Menü **Aktion**. Danach wird der Aufgaben-Assistent gestartet, der dem Assistenten für Erstellung lokaler Aufgaben

gleicht (Näheres s. Pkt. 6.3.1.1 auf S. 173). Befolgen Sie dessen Hinweise.

Nachdem der Assistent seine Arbeit beendet hat, wird die Aufgabe im Ordner **Gruppentasks** der entsprechenden Gruppe für alle in diese eingebetteten Gruppen abgelegt und in der Ergebnisleiste angezeigt.

6.3.1.3. Erstellung einer globalen Aufgabe

Um eine globale Aufgabe für Kaspersky Anti-Virus n, gehen Sie wie folgt vor:

1. Wählen Sie im Konsoleverzeichnis den Knoten **Globale Tasks** aus, rufen Sie das Kontextmenü auf und wählen Sie den Befehl **Neu→ Task** aus oder benutzen Sie den gleichen Punkt im Menü **Aktion**.
2. Danach wird der Aufgaben-Assistent gestartet, der dem Assistenten für Erstellung lokaler Aufgaben gleicht (Näheres s. Pkt. 6.3.1.1 auf S. 173). Abweichend davon ist die Stufe vorhanden, wo die einzelnen Clients des logischen Netzes auszuwählen sind, für die globale Aufgabe laufen wird.
3. Wählen Sie Clients des logischen Netzes aus, auf welchen die Aufgabe laufen wird. Sie können Clients aus verschiedenen Ordnern wählen. Es kann auch der ganze Ordner gewählt werden (Näheres siehe Hilfesystem für Kaspersky Administration Kit 5.0).

Globale Aufgaben werden nur für einen festgesetzten Satz von Computern ausgeführt. Werden zu einer Gruppe von Rechnern, für die Aufgabe der Ferninstallation definiert wurde, weitere Computer hinzugefügt, so wird für die hinzugefügten Rechner die Aufgabe nicht ausgeführt. Dazu ist eine neue Aufgabe zu erstellen oder die bestehende Aufgabe dementsprechend zu ändern.

Nachdem der Assistent seine Arbeit beendet hat, wird die globale Aufgabe zum Knoten **Tasks** des Konsoleverzeichnisses hinzugefügt und in der Ergebnisleiste angezeigt.

6.3.2. Anzeige und Korrektur der Aufgabeneinstellungen. Verfolgung der Ausführung

Um Einstellungen für eine Aufgabe anzusehen bzw. zu korrigieren, gehen Sie wie folgt vor:

- Geht es um eine lokale Aufgabe, dann wählen Sie aus dem Ordner **Gruppen** den Ordner mit dem Namen der Gruppe, zu welcher der betreffende Client gehört. Wählen Sie den benötigten Computer aus der Ergebnisleiste aus und benutzen Sie den Befehl **Eigenschaften** im Kontextmenü. Im angezeigten Dialogfeld **Eigenschaften von <Computername>** wechseln Sie in die Registerkarte **Tasks** (siehe Abbildung 95). Anzeige und Korrektur der Einstellungen für die gewählte Aufgabe erfolgt im Fenster, das sich über die Schaltfläche **Eigenschaften** öffnet.

  In der Registerkarte **Aufgaben** finden Sie die vollständige Auflistung der Aufgaben für einen lokalen Rechner (u.a. globale und Gruppen-Aufgaben). Globale und Gruppenaufgaben werden mit dem Symbol "Ordner" kenntlich gemacht. Sie können die Parameter aller Aufgaben einsehen, es können aber nur lokale Aufgaben editiert werden.

- Geht es um eine Gruppenaufgabe, dann wählen Sie aus dem Konsoleverzeichnis die betreffende Gruppe und anschließend den dazugehörigen Ordner **Gruppenaufgaben** aus. Ferner erscheint in der Ergebnisleiste die Auflistung aller für diese Gruppe erstellten Aufgaben. Wählen Sie die gewünschte Aufgabe aus, rufen Sie das Kontextmenü auf und wählen Sie den Befehl **Eigenschaften** aus oder benutzen Sie den gleichen Punkt im Menü **Aktion**.

- Möchten Sie die Einstellungen für eine globale Aufgabe ändern, dann wählen Sie im Konsoleverzeichnis den Knoten **Globale Tasks** und anschließend die gewünschte Aufgabe aus, rufen Sie das Kontextmenü auf und wählen Sie den Befehl ***Eigenschaften*** aus oder benutzen Sie den gleichen Punkt im Menü **Aktion**.

Darauf erscheint das Dialogfeld mit den Aufgabeneinstellungen **Eigenschaften: Name der Aufgabe** mit folgenden Registerkarten: **Allgemein**, **Einstellungen**, **Benutzerkonto**, **Zeitplan**, **Benachrichtigung**. Das Dialogfeld zur Einstellung einer globalen Aufgabe enthält auch die Registerkarte **Zielcomputer**, für welche die Aufgabe erstellt wird.

Alle Registerkarten (außer **Einstellungen** und **Benutzerkonto**) sind standardmäßige Registerkarten zur Einstellung von Aufgaben für Kaspersky Administration Kit 5.0. Deren detaillierte Beschreibung finden Sie im gleichnamigen Handbuch für Administratoren. In der Registerkarte **Einstellungen** finden Sie spezifische Einstellungen für Kaspersky Anti-Virus 5.0 for Windows Workstations. Der Inhalt dieser Registerkarte hängt vom gewählten Aufgabentyp ab (s. Schritt 3. auf S. 175). Auf der Registerkarte **Benutzerkonto** wird der Aufgabenstart unter einem bestimmten Benutzerkonto konfiguriert (s. Pkt. 5.9 auf S. 110).

6.3.3. Starten und Beenden von Aufgaben

Aufgaben werden auf einzelnen Clients nur dann gestartet, wenn die entsprechende Anwendung gestartet wurde. Wird die Anwendung angehalten, so werden auch alle gestarteten Aufgaben nicht mehr ausgeführt.

Aufgaben werden automatisch gestartet und beendet (gemäß Zeitplan). Dies kann auch manuell (aus dem Kontextmenü) und auch aus der Einstellungsvorschau für Aufgaben erfolgen. Sie können die Ausführung einer gestarteten Aufgabe anhalten und fortsetzen.

Um eine Aufgabe manuell zu starten / anzuhalten / unterbrechen / wieder fortzuführen:

Wählen Sie die gewünschte Aufgabe aus, rufen Sie das Kontextmenü auf und wählen Sie den Befehl **Starten / Beenden** aus oder benutzen Sie die gleichen Punkte im Menü **Aktion**.

Ähnliche Aktionen können Sie aus dem Dialogfeld mit Aufgabeneinstellungen in der Registerkarte **Allgemein** mit Hilfe von gleichnamigen Schaltflächen einleiten (s. Pkt. 6.3.2 auf S. 180).

6.4. Verwaltung der Programmeinstellungen

Mit Hilfe der Programmeinstellungen können Sie die Parameter des Programmbetriebs für einzelne Clients einer Gruppe ändern. Geändert können nur diejenigen Parameter, deren Modifizierung durch die Richtlinie für diese Anwendung nicht gesperrt ist.

Um Programmeinstellungen zu ändern:

1. Wählen Sie im Ordner **Gruppen** den Ordner mit dem Namen der Gruppe, zu welcher der betreffende Client gehört.
2. Wählen Sie aus der Ergebnisleiste den Rechner aus, für welchen die Programmeinstellungen zu ändern sind, und benutzen Sie den Kontextmenü-Befehl **Eigenschaften** oder den gleichen Punkt im Menü **Aktion**.
3. Danach erscheint im Programmhauptfenster das aus vier Registerkarten bestehende Dialogfeld **Eigenschaften von <Computername>**. Wechseln Sie in die Registerkarte **Anwendungen** (s. Abbildung 99). Hier finden Sie die vollständige Auflistung aller Anwendungen des Kaspersky Lab, die auf dem betreffenden Client laufen.

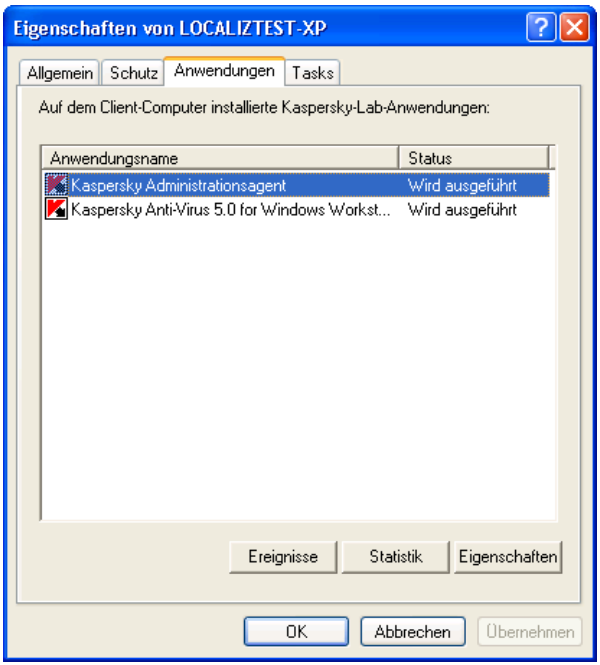

Abbildung 99. Vorschau der Clienteigenschaften. Registerkarte **Anwendungen**

4. Wählen Sie **Kaspersky Anti-Virus 5.0 for Windows Workstations**. Unter der Liste sind Schaltflächen angeordnet (**Ereignisse**, **Statistik**, **Eigenschaften**), mit denen Sie folgende Aktionen ausführen können:

   - Ereignisse ansehen, die während des Anwendungbetriebs auf dem betreffenden Client eingetreten sind und vom Verwaltungsserver registriert wurden (über die Arbeit mit Reports siehe Hilfesystem Kaspersky Administration Kit 5.0).
   - aktuelle Statistiken zum Anwendungsbetrieb ansehen.
   - **Eigenschaften** – Einstellung der Anwendung. Beim Mausklick auf diese Schaltfläche wird ein Dialogfeld mit folgenden Registerkarten aufgerufen: **Allgemein**, **Zusätzliches**, **Bedrohungen und Ausnahmen**, **Vertrauenswürdige Prozesse**, **Quarantäne**, **Backup**, **Objekte des Backups**, **Lizenzen**, **Ereignisbearbeitung**. Diese Registerkarten sind unten ausführlich beschrieben.

6.4.1. Anzeige der Informationen über Anwendung

In der Registerkarte **Allgemein** (s. Abbildung 100) können Sie allgemeine Informationen zu Kaspersky Anti-Virus 5.0 for Windows Workstations einsehen, das Programm starten oder anhalten.

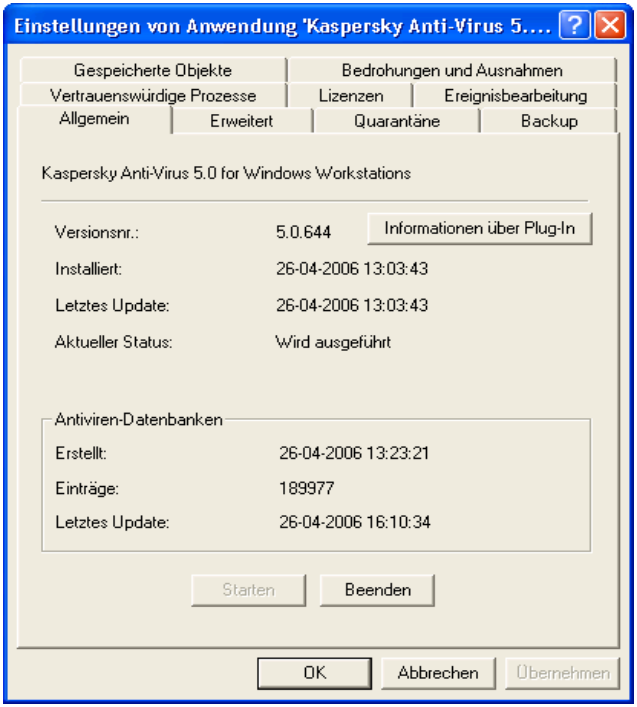

Abbildung 100. Fenster der Anwendungseigenschaften.
Registerkarte **Allgemein**

Im oberen Teil des Dialogfeldes befindet sich der Name der installierten Anwendung, Angaben zur Version, Installationsdatum und Status (ob die Anwendung auf dem lokalen Rechner gestartet ist oder angehalten wurde) sowie Informationen über den Zustand der Antiviren-Datenbanken.

Mit den entsprechenden Schaltflächen können Sie die Anwendung starten oder beenden.

Mit Hilfe der Schaltfläche **Informationen über Plug-In** können Sie allgemeine Informationen über das Plugin zur Verwaltung der Anwendung Kaspersky Anti-Virus 5.0 for Windows Workstations anzeigen (s. Abb. 101).

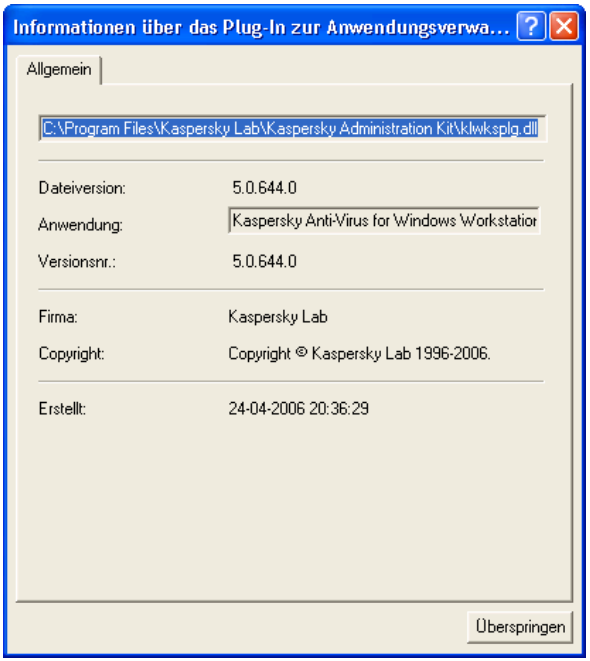

Abbildung 101. Informationen zum Plugin für die Anwendungsverwaltung

6.4.2. Zusatzeinstellungen der Anwendung

Mit den Registerkarten **Zusätzliches**, **Quarantäne**, **Zugelassene Programme**, **Vertrauenswürdige Prozesse** und **Backup** können Sie die Parameter des Kaspersky Anti-Virus 5.0 for Windows Workstations auf einem Fernrechner einstellen.

Diese Einstellungen entsprechen den Einstellungen der Gruppenrichtlinie (Näheres s. Pkt. 6.2.2 auf S. 142).Dabei sind die Einstellungen der Richtlinie für die Einstellungen der Anwendung maßgebend.

Bei der Programmkonfiguration auf einem lokalen Computer können Sie nur die Werte ändern, deren Änderung durch die Gruppenrichtlinie freigegeben ist.

6.4.3. Arbeiten mit Quarantäne und Backup

Kaspersky Anti-Virus 5.0 für Windows Workstations unterstützt die Funktion der Speicherung von infizierten und verdächtigen Objekten und ihrer Backup-Kopien in speziellen Ablagen.

Für jeden Rechner gibt es individuelle Quarantäne- und Backup-Ablagen, die sich lokal auf dem betreffenden Rechner befinden.

Um sich die in der Quarantäne- bzw. Backup-Ablage eines Rechners befindlichen Objekte anzusehen, wechseln Sie in die Registerkarte **Objekte des Backups** (s. Abbildung 102).

Dazu klicken Sie die Schaltfläche **Objektliste** in den Bereichen **Quarantäne** oder **Backup** an.

Kann die Anwendung keine Verbindung zum Client aufbauen, so erscheint auf dem Bildschirm ein Dialogfeld mit dem Vorschlag, den Versuch zu wiederholen oder auf die Verbindung zu verzichten.

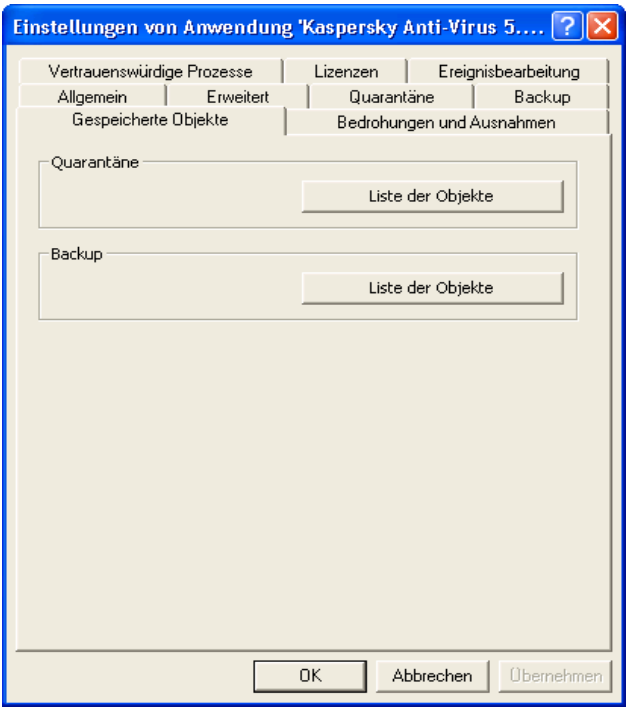

Abbildung 102. Registerkarte **Gespeicheite Objekte**

Die Dialogfenster beider Ablagen sehen gleich aus (siehe Abbildung 103). Im zentralen Bereich des Dialogfeldes sehen Sie die Liste von in Quarantäne verschobenen Objekten oder die Liste der Backup-Kopien. Für jedes Objekt werden folgende Informationen angezeigt: Name, Objektstatus, Datum für das Verschieben in den Backup und Ausgangspfad.

Über der Liste befindet sich die Verwaltungsleiste zur Verwaltung von Objekten in Quarantäne bzw. in der Backup-Ablage. Sie enthält folgende Schaltflächen:

– Objekt wiederherstellen; beim Anklicken öffnet sich ein Dialogfeld, in dem der Pfad zum Zielordner einzugeben ist, in dem das Objekt wiederherzustellen ist.

Bei der Fernsteuerung mittels Kaspersky Administration Kit wird die Wiederherstellung der Objekte nur auf dem Computer durchgeführt, wo die *Administrierungskonsole* installiert wird.

– Objekt aus der Ablage löschen.

– Ablageninhalt aktualisieren.

– Objektuntersuchung starten (nur für Quarantäne).

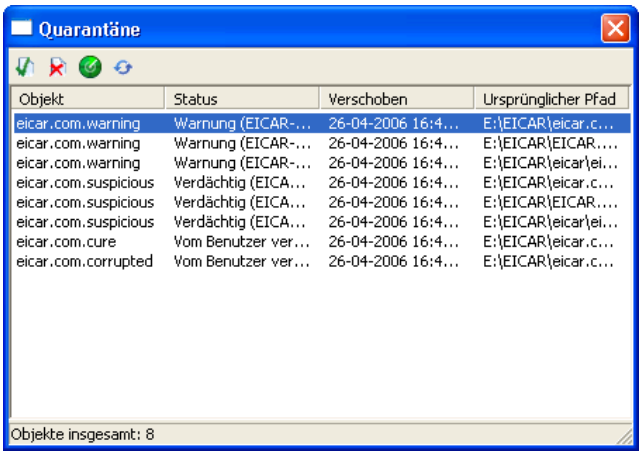
Quarantäne
Objekt
Status
Verschoben
Ursprünglicher Pfad
eicar.com.warning Warnung (EICAR-... 26-04-2006 16:4... E:\EICAR\eicar.c...
eicar.com.warning Warnung (EICAR-... 26-04-2006 16:4... E:\EICAR\EICAR....
eicar.com.warning Warnung (EICAR-... 26-04-2006 16:4... E:\EICAR\eicar\ei...
eicar.com.suspicious Verdächtig (EICA... 26-04-2006 16:4... E:\EICAR\eicar.c...
eicar.com.suspicious Verdächtig (EICA... 26-04-2006 16:4... E:\EICAR\EICAR....
eicar.com.suspicious Verdächtig (EICA... 26-04-2006 16:4... E:\EICAR\eicar\ei...
eicar.com.cure Vom Benutzer ver... 26-04-2006 16:4... E:\EICAR\eicar.c...
eicar.com.corrupted Vom Benutzer ver... 26-04-2006 16:4... E:\EICAR\eicar.c...
Objekte insgesamt: 8

Abbildung 103. Quarantäne

6.4.4. Anzeige der Information über Lizenzschlüssel

Die Registerkarte **Lizenzen** (siehe Abbildung 104) hat lediglich einen informativen Charakter. Hier finden Sie Angaben zum aktuellen Lizenzschlüssel und Reserveschlüssel, die auf einem konkreten Client installiert sind.

Abbildung 104. Registerkarte **Lizenzen**

6.4.5. Einstellungen der Optionen der Protokollerstellung

In der Registerkarte **Ereignissen** können Sie die Parameter für Verschicken von Meldungen über den Betrieb des Anti-Virus von einem Fernrechner aus einstellen.

Die Einstellungen in dieser Registerkarte entsprechen den Einstellungen der gleichnamigen Registerkarte der Gruppenrichtlinie (Näheres s. Pkt. 6.2.2.13 auf S. 164).

KAPITEL 7. TESTEN DER KORREKTEN FUNKTION VON KASPERSKY ANTI-VIRUS

7.1. „Testvirus“ EICAR und seine Modifikationen

Nach Installation und Einstellung des Kaspersky Anti-Virus wird empfohlen, die richtige Einstellung und die korrekte Arbeit der Software mithilfe eines „Testvirus“ und dessen Modifikationen zu untersuchen.

Dieses „Testvirus“ wurde vom Institut eicar (The European Institute for Computer Antivirus Research) zum Testen der Funktionsweise von Antiviren-Software entwickelt.

Das „Testvirus“ IST KEIN SCHÄDLING und enthält keinen Programmcode, der Ihren Rechner beschädigen könnte. Dabei wird es von den meisten Softwareprodukten der Antivirus-Hersteller als Virus erkannt.

Verwenden Sie nie echte Viren, um die Funktionsweise von Antiviren-Software zu testen!

Das „Testvirus“ kann von der offiziellen Internet-Präsenz des Instituts **EICAR** heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm. Sollten Sie keinen Internetzugang haben, dann können Sie ein „Tesevirus2 selbst schreiben. Dazu tippen Sie in einem beliebigen Texteditor folgende Zeile und speichern Sie diese in einer Datei mit dem Namen **eicar.com** ab:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Die von der Web-Seite des **EICAR**-Instituts heruntergeladene bzw. von Ihnen wie oben beschrieben selbst erstellte Datei enthält den Code eines standardmäßigen „Testvirus“. Kaspersky Anti-Virus erkennt diese Datei, weist ihr den Typ **Infiziert** zu und führt die durch den Administrator für solchen Objekttyp festgelegte Aktion aus.

Um die Reaktion des Kaspersky Anti-Virus beim Auffinden von Objekten anderen Typs zu untersuchen, können Sie den Inhalt des standardmäßigen „Testvirus“ durch zusätzliche Angabe eines Präfixes modifizieren (s. Tabelle 3“).

Sie können die korrekte Funktion des Kaspersky Anti-Virus mithilfe des modifizierten EICAR-Virus nur dann untersuchen, wenn Ihnen nach dem 24.10.2003 erstellte Antiviren-Datenbanken zur Verfügung stehen (kumulative Aktualisierung – Oktober 2003).

Tabelle 3. „Testvirus-Modifikationen“

Präfix	Objekttyp
kein Präfix, standard-mäßiges Testvirus	**Infiziert**. Beim Säuberungsversuch tritt ein Fehler auf; Objekt wird gelöscht.
CORR–	**Beschädigt**.
SUSP–	**Verdächtig** (unbekannter Virus-Code).
WARN–	**Verdächtig** (modifizierter Code eines bekannten Virus).
ERRO–	**Wegen Störung nicht untersucht.**
CURE–	**Infiziert**. Objekt wird gesäubert. Dabei ändert sich der Inhalt des Virustextes in CURE.
DELE–	**Infiziert**. Das Objekt wird automatisch gelöscht.

Die erste Spalte dieser Tabelle enthält Präfixe, die beim standardmäßigen „Testvirus“ am Zeilenanfang hinzuzufügen sind (z.B. DELE–X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*).

Nachdem Sie das Präfix zum „Testvirus“ hinzugefügt haben, speichern Sie das Virus in einen Datei z.B. namens eicar_dele.com ab (ähnlicherweise sind auch alle anderen Virusmodifikationen zu benennen).

In der zweiten Spalte sind Objekttypen beschrieben, die von Kaspersky Anti-Virus nach zusätzlicher Angabe von Präfixen identifiziert werden. Aktionen mit jedem Objekt werden durch die vom Administrator vorgegebenen Einstellungen bestimmt.

7.2. Testen der Funktion von Kaspersky Anti-Virus

Zur Untersuchung der richtigen Einstellung und der korrekten Arbeit von Kaspersky Anti-Virus 5.0 for Windows Workstation,

- Legen Sie auf der Festplatte ein Verzeichnis an und speichern Sie darin die von Ihnen geschriebenen „Testviren".
- Erstellen Sie eine benutzerdefinierte Aufgabe und stellen Sie diese ein (s. Pkt. 5.6 auf S. 101).
    - Fügen Sie das Verzeichnis, das abgelegte „Testviren" enthält, in die Liste der bei Ausführung der Aufgabe zu untersuchenden Objekte hinzu.
    - Als Aktion von Kaspersky Anti-Virus beim Erkennen infizierter oder verdächtiger Objekte wählen Sie die Variante *Benutzer nach Aktion fragen* aus.
- Im Dialog **Zusatzeinstellungen** (s. Pkt. 5.10.4 auf S. 125) setzen Sie das Häkchen **Alle Protokolle speichern**. Dies ist notwendig, damit in der Report-Datei Daten über beschädigte oder wegen einer Beschädigung nicht untersuchte Dateien abgespeichert werden können.
- Starten Sie die Ausführung der Aufgabe.

Sobald während der Untersuchung verdächtige oder infizierte Objekte erkannt werden, erscheinen auf dem Bildschirm Dialoge mit Informationen zum Objekt und der Frage an den Benutzer, welche Aktion vorzunehmen ist. So erscheint beispielsweise beim Auffinden eines Objekts mit dem SUSP-Präfix folgende Meldung:

Kaspersky Anti-Virus fur Windows Workstations
Achtung! Ein Objekt wurde gefunden, das möglicherweise von einem Virus infiziert ist.
Objekt E:\...\eicar.com.suspicious ist möglicherweise infiziert von Virus EICAR-Test-File. Wir empfehlen das Verschieben dieses Objekts nach Quarantäne.
Nach Quarantäne verschieben (empfohlen)
Löschen
Überspringen
Anwenden auf alle möglicherweise infizierten Objekte, deren Desinfektion nicht möglich ist (während dieser Sitzung)
Hilfe
Tonsignale AUS
OK

Abbildung 105. Achtung! Verdächtiges Objekt gefunden

Auf diese Weise können Sie durch Auswahl von verschiedenen Aktionsvarianten in den während der Untersuchung erscheinenden Dialogen die Reaktion von Kaspersky Anti-Virus beim Auffinden von Objekten verschiedenen Typs untersuchen.

Der komplette Untersuchungsergebnis wird im Ergebnisbericht dargestellt (s. Abbildung 106).

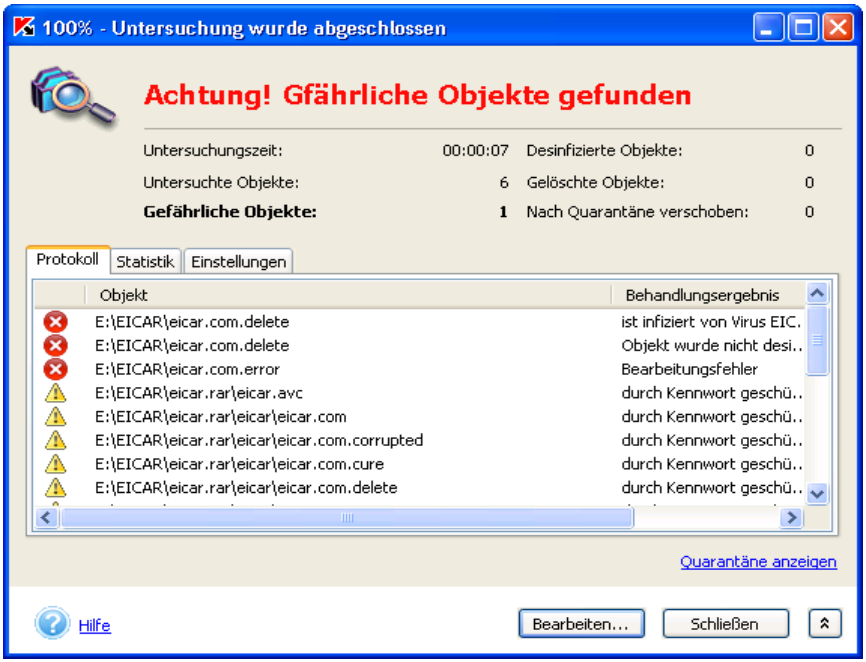

Abbildung 106. Report über die Untersuchung des Verzeichnisses mit den „Testviren“

KAPITEL 8. VERWALTUNG DER LIZENZSCHLÜSSEL

Sie können Kaspersky Anti-Virus erst nach der Installation des *Lizenzschlüssels* verwenden, der zum Lieferumfang des Produkts gehört.

Kaspersky Anti-Virus for Windows Workstations FUNKTIONIERT NICHT ohne Lizenzschlüssel!

Mit Ablauf der Lizenzgültigkeit bleibt die Funktionalität von Kaspersky Anti-Virus unter Ausnahme der Update-Möglichkeit der Antiviren-Datenbanken erhalten. Sie können Ihren Computer und Ihre E-Mails weiterhin auf das Vorhandensein von Viren untersuchen und gefährliche Objekte desinfizieren, dabei aber nur die Antiviren-Datenbanken verwenden, die am Datum des Ablaufs der Lizenz aktuell waren. Demzufolge können wir Ihnen keinen hundertprozentigen Antivirenschutz vor neuen Viren garantieren, die nach dem Ende der Lizenzgültigkeit für Kaspersky Anti-Virus auftreten.

Um eine Infektion Ihres Computers durch neue Viren zu verhindern, empfehlen wird Ihnen, die Lizenz für die Benutzung von Kaspersky Anti-Virus zu verlängern.

Zwei Wochen vor Ablauf der Lizenzgültigkeit werden Sie von Kaspersky Anti-Virus darüber benachrichtigt. Innerhalb dieser zwei Wochen wird bei jedem Programmstart eine entsprechende Meldung auf dem Bildschirm angezeigt.

Um die Lizenz zu verlängern, ist der Erwerb und die Installation eines neuen Lizenzschlüssels für Kaspersky Anti-Virus erforderlich. Folgen Sie dazu dieser Beschreibung:

1. Wenden Sie sich an den Händler, bei dem Sie die Software erworben haben und erwerben Sie einen Lizenzschlüssel für die Nutzung von Kaspersky Anti-Virus 5.0 for Windows Workstations.

oder:

Erwerben Sie direkt bei Kaspersky Lab einen Lizenzschlüssel. Verwenden Sie dazu den Hyperlink Lizenz erneuern auf der Registerkarte **Support** (s. Abbildung 4) oder die Schaltfläche **Verlängern** im Fenster **Verwaltung der Lizenzschlüssel** (s. Abbildung 107). Dadurch wird unsere Webseite geöffnet. Füllen Sie dort das entsprechende Formular aus. Nach Eingang der Bezahlung wird Ihnen per E-Mail ein Link an die im Bestellformular angegebene Adresse zugeschickt. Über diesen Link können Sie den Lizenzschlüssel herunterladen.

2. Installieren Sie den Lizenzschlüssel. Näheres zur Arbeit mit den Lizenzschlüsseln über die lokale Lizenzschlüssel-Schnittstelle siehe Pkt. 8.1 auf S. 196, über die Schnittstelle des Kaspersky Administration Kit 5.0 - siehe Pkt. 8.2 auf S. 199.

Sie können zwei Schlüssel installieren: einen aktiven und einen Reserve-Schlüssel. Der aktive Schlüssel gilt für einen bestimmten Zeitraum. Das Programm kann nur einen Schlüssel mit dem Status "aktiv" besitzen. Die Gültigkeitsdauer des Reserve-Schlüssels beginnt unmittelbar, nachdem der aktive Schlüssel abgelaufen ist.

8.1. Verwaltung der Lizenzschlüssel über die lokale Benutzeroberfläche:

Um die Lizenz während der Arbeit über eine lokale Schnittstelle des Kaspersky Anti-Virus for Windows Workstations zu verlängern, gehen Sie wie folgt vor:

1. Erwerben Sie einen Lizenzschlüssel (Details s. oben).
2. Installieren Sie den Lizenzschlüssel wie folgt:
   a. Verwenden Sie den Hyperlink Lizenzschlüssel auf der linken Seite der Registerkarte **Support** (s. Abbildung 4).
   b. Klicken Sie im Fenster **Verwaltung der Lizenzschlüssel** (s. Abbildung 107) auf die Schaltfläche **Hinzufügen**.
   c. Gehen Sie im Standardfenster zur Dateiauswahl zum Ordner, in dem sich der Lizenzschlüssel befindet (Datei mit der Erweiterung **.key**). Wählen Sie den gewünschten Schlüssel und klicken Sie auf die Schaltfläche **Öffnen**.
   d. Lesen Sie im folgenden Fenster **Schlüssel aktivieren** (s. Abb. 108) die Informationen über den Schlüssel, der hinzugefügt werden soll, und klicken Sie auf die Schaltfläche **Aktivieren**, um ihn zu aktivieren.

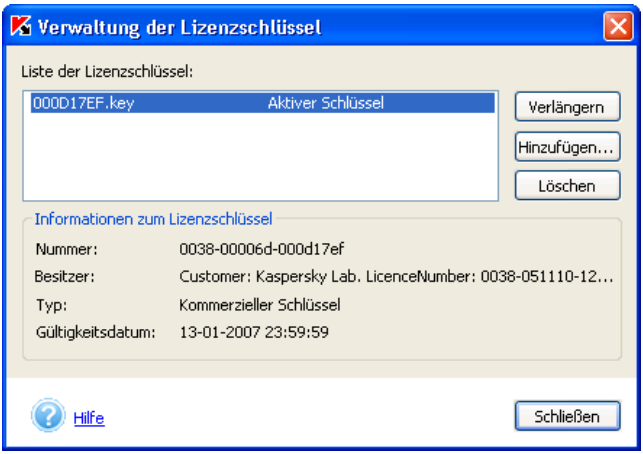

Abbildung 107. Fenster **Verwaltung der Lizenzschlüssel**

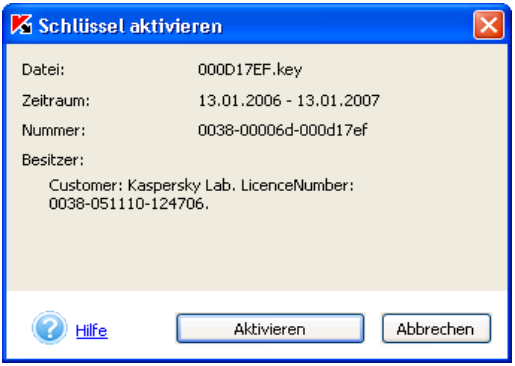

Abbildung 108. Fenster zum Aktivieren des Schlüssels

oder:

a. Wählen Sie im Menü **Start** → **Programme** die Gruppe Kaspersky Anti-Virus und im Dropdown-Menü den Punkt **Lizenzschlüssel installieren**.

b. Klicken Sie im folgenden Fenster auf die Schaltfläche **Durchsuchen** und gehen Sie zum Ordner, in dem sich der Lizenzschlüssel befindet.

c. Wählen Sie den gewünschten Lizenzschlüssel und klicken Sie auf die Schaltfläche **Öffnen**.

d. Aktivieren Sie im unteren Teil des Fensters (s. Abbildung 109) das Kontrollkästchen neben dem Namen der Anwendung, für welche Sie den Lizenzschlüssel installieren möchten. Klicken Sie auf die Schaltfläche **OK**.

Wenn die Liste im unteren Teil des Fensters leer ist, dann passt der gewählte Lizenzschlüssel zu keiner der Kaspersky-Lab-Anwendungen, die auf Ihrem Computer installiert sind.

Wählen Sie einen anderen Lizenzschlüssel.

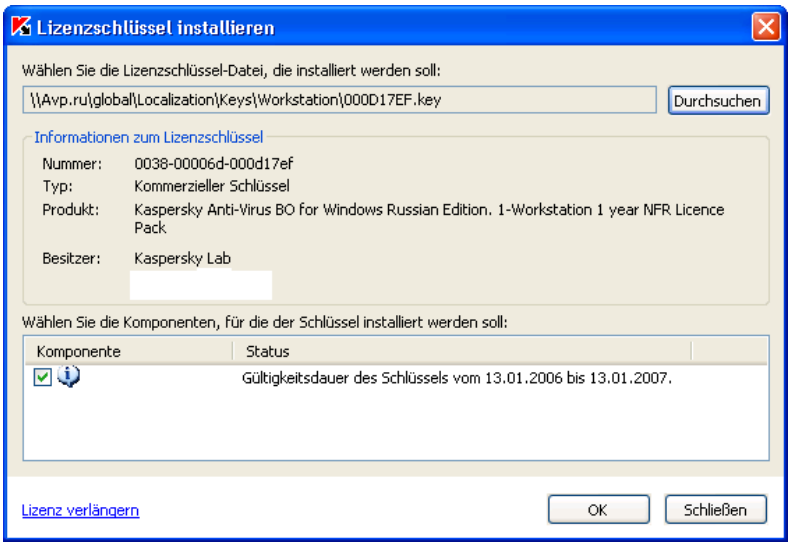

Abbildung 109. Fenster **Installation des Lizenzschlüssels**

e. Lesen Sie im folgenden Fenster **Aktivierung des Lizenzschlüssels** (s. Abbildung 108) die Informationen über den hinzugefügten Schlüssel und klicken Sie auf die Schaltfläche **Aktivieren**, um den Schlüssel zu verwenden.

Wenn Sie einen neuen Schlüssel hinzufügen, während noch ein gültiger aktiver Schlüssel vorhanden ist, werden Ihnen zwei Installationsvarianten angeboten:

- Neuen Schlüssel als Reserveschlüssel speichern (empfohlen). Bei Auswahl dieser Variante wird der Schlüssel mit dem Status *Reserve* zur Liste hinzugefügt. Bei Ablauf des aktiven Schlüssels erhält der neue Schlüssel automatisch den Status *aktiver Schlüssel*.

- Aktiven Schlüssel durch neuen ersetzen. Bei Auswahl dieser Variante wird der neue Schlüssel mit dem Status „aktiver Schlüssel“ zur Liste hinzugefügt.

Beachten Sie, dass beim Löschen des aktiven Schlüssels auch der installierte Reserve-Schlüssel automatisch gelöscht wird!

8.2. Verwaltung der Lizenzschlüssel über die Schnittstelle Kaspersky Administration Kit

Bei Verwaltung über Kaspersky Administration Kit 5.0 haben Sie zwei Möglichkeiten, die Lizenz zu verlängern:

- *Lizenz gruppenweise hinzufügen* – die Lizenz für Kaspersky Anti-Virus wird gleichzeitig für die ausgewählten Computer oder Gruppen von Client-Computern verlängert. Dazu dienen globale oder Gruppenaufgaben (Details s. Hilfesystem für Kaspersky Administration Kit 5.0).
- *Lizenz individuell hinzufügen* – die Lizenz für Kaspersky Anti-Virus wird nur für einen gewählten Computer verlängert.

Um die Lizenz für eine einzelne Workstation zu verlängern, haben Sie einen neuen Lizenzschlüssel für Kaspersky Anti-Virus zu erwerben und zu installieren. Gehen Sie hierzu wie folgt vor:

1. Erwerben Sie einen Lizenzschlüssel (Näheres s. Kapitel 8 auf S. 195).
2. Erstellen Sie eine Aufgabe zur Installation des Lizenzschlüssels (s. Pkt. 6.3.1.1 auf S. 173).

Informationen über Lizenzschlüssel (aktive und Reserveschlüssel), die an einem einzelnen Rechner installiert sind, finden Sie in der Registerkarte **Lizenzen** (Näheres s. Pkt. 6.4.4 auf S. 188).

KAPITEL 9. STEUERUNG DER ANWENDUNG MIT HILFE DER BEFEHLSZEILE

Kaspersky Anti-Virus kann mit Hilfe des Dienstprogramms **kavshell.exe**, das zur Produktdistribution gehört, aus der Befehlszeile gesteuert werden. Dieses Dienstprogramm befindet sich nach der Installation von Kaspersky Anti-Virus im Stamm des Programminstallationsverzeichnisses. Beim Start des Dienstprogramms aus der Befehlszeile stehen in Abhängigkeit von den verwendeten Befehlen folgende Funktionen zur Verfügung:

SCAN	Untersuchung von ausgewählten Objekten
FULLSCAN	vollständige Untersuchung des Computers
UPDATE	Aktualisierung der Antiviren-Datenbanken und Anwendungsmodule
ROLLBACK	Rückgängigmachen des letzten Updates der Antiviren-Datenbanken
RTP	Steuerung des Echtzeitschutzmodus für den Computer
START	Start von Kaspersky Anti-Virus
STOP	Beenden von Kaspersky Anti-Virus
TASK	Steuerung von Aufgaben für Kaspersky Anti-Virus
IMPORT	Importieren von Einstellungen für Kaspersky Anti-Virus aus einer Datei
EXPORT	Exportieren von Einstellungen für Kaspersky Anti-Virus in eine Datei

ADDKEY	Hinzufügen eines Lizenzschlüssels

Wenn in Kaspersky Anti-Virus die Verwendung des Benutzer- und Administratormodus nicht aktiviert ist (s. Pkt. 5.10.7 auf S. 131), werden Befehle, die ein Kennwort erfordern, nicht ausgeführt. In diesem Fall wird eine Fehlermeldung angezeigt.

Verwenden Sie zur Anzeige der Befehlssyntax:

```
KAVSHELL HELP [Befehl]
KAVSHELL [Befehl] /?
```

[7]

Wenn der Schlüssel **Befehl** nicht festgelegt wurde, wird eine Liste aller verfügbaren Befehle angezeigt.

Beispiele:

```
KAVSHELL HELP SCAN
KAVSHELL SCAN /?
```

9.1. Untersuchung ausgewählter Objekte

Befehlssyntax:

```
KAVSHELL SCAN [Objekte] [/L[!]:Datei_der_Objekte] [/F(A|E|C)]
[/NP] [/ASK | /DISINFECT|/DELETE] [/W[A][!]:Protokolldatei]
```

Wenn keiner der Schlüssel angegeben wird, erscheinen Hilfeinformationen zur Befehlssyntax.

Die Untersuchungsaufgabe wird mit den Einstellungen ausgeführt, die von den Kaspersky-Lab-Experten empfohlen werden.

Schlüssel	Funktion
Objekte	Gibt eine Liste aus einer oder mehreren Dateien, Ordnern oder vordefinierten Objekten an, die durch

[7] Optionale Schlüssel stehen in eckigen Klammern.

	Ordnern oder vordefinierten Objekten an, die durch Leerzeichen getrennt werden. Vordefinierte Objekte können sein: • **/MEMORY** – Systemspeicher • **/STARTUP** – Autostart-Objekte • **/MAIL** – Mailboxen für Microsoft Office Outlook und Microsoft Outlook Express • **/REMDRIVES** – Wechsellaufwerke • **/FIXDRIVES** – Festplatten • **/NETDRIVES** – Netzlaufwerke Kommentare: • Wenn der Name eines Objekts ein Leerzeichen enthält, muss er in Anführungszeichen gesetzt werden. • Zur Untersuchung mehrerer Dateien können Masken benutzt werden (Beispiele für Masken s. Pkt. 5.7 auf S. 102). • Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
/L[!]:Datei_der_Objekte	Gibt eine Datei im Format **.txt** an, die eine Liste der zu untersuchenden Objekte (Dateien, Ordner, vordefinierte Objekte) enthält. Jeder Objektname muss in dieser Datei in einer separaten Zeile stehen. Das Zeichen **!** bedeutet, dass die Datei nach dem Untersuchungsabschluss aus der Liste gelöscht wird. Die Angabe des absoluten oder relativen Dateipfads ist zulässig. Der Pfad wird in Anführungszeichen gesetzt, wenn er ein Leerzeichen enthält.
/F(A|E|C) **/FA** **/FC** **/FE**	Typen der zu untersuchenden Dateien: • alle Dateien untersuchen. • infizierbare Dateien nach Format untersuchen. • infizierbare Dateien nach Erweiterung untersuchen.

/NP	Kennwortgeschützte Objekte überspringen.
• **/ASK** • **/DISINFECT** • **/DELETE**	Aktion für ein infiziertes Objekt: • Benutzer nach Aktion fragen. • Desinfizieren, irreparable Objekte löschen. • Löschen. Kommentare: • Wenn keine Aktion angegeben wird, wird das Objekt übersprungen und Informationen über den Fund werden protokolliert. • Zusammengesetzte Dateien werden nicht gelöscht.
/W[A][!]:Protokolldatei • **/W:Protokolldatei** • **/WA:Protokolldatei**	Protokollieren von Ereignissen in der angegebenen **Protokolldatei**: • nur wichtige Ereignisse • alle Ereignisse Das Zeichen **!** bedeutet, dass die Protokolldatei nach jedem Aufgabenstart überschrieben wird. Die Angabe des absoluten oder relativen Dateipfads ist zulässig. Der Pfad wird in Anführungszeichen gesetzt, wenn er ein Leerzeichen enthält.

Beispiele:

```
KAVSHELL SCAN "C:\Program Files" C:\Downloads\test.exe
/MEMORY /STARTUP /FA /DISINFECT /WA:log.txt
KAVSHELL SCAN /MEMORY /STARTUP C:\Downloads\test.exe /FC
/W:log.txt /ASK
```

9.2. Vollständige Untersuchung

Befehlssyntax:

```
KAVSHELL FULLSCAN [/W[A][!]:Protokolldatei] [/D]
```

Wenn keiner der Schlüssel angegeben wird, erscheinen Hilfeinformationen zur Befehlssyntax.

Die Untersuchungsaufgabe wird mit den Einstellungen ausgeführt, die von den Kaspersky-Lab-Experten empfohlen werden.

Schlüssel	Funktion
/W[A][!]:Protokolldatei • **/W:Protokolldatei** • **/WA:Protokolldatei**	Protokollieren von Ereignissen in der angegebenen Protokolldatei: • nur wichtige Ereignisse • alle Ereignisse Das Zeichen **!** bedeutet, dass die Protokolldatei nach jedem Aufgabenstart überschrieben wird. Die Angabe des absoluten oder relativen Dateipfads ist zulässig. Der Pfad wird in Anführungszeichen gesetzt, wenn er ein Leerzeichen enthält.
/D	Die Untersuchung wird verworfen, wenn sie am selben Tage bereits erfolgreich ausgeführt wurde.

Beispiele:

```
KAVSHELL FULLSCAN /WA:fullscan.log
```

9.3. Updatestart

Befehlssyntax:

```
KAVSHELL UPDATE [Update-Quelle] [/W[A][!]:Protokolldatei]
[/APP]
```

Wenn keiner der Schlüssel angegeben wird, erscheinen Hilfeinformationen zur Befehlssyntax.

Schlüssel	Funktion
[**Update-Quelle**]	HTTP-, FTP-Server oder Netzwerkordner für den Update-Download. Wenn kein Pfad angegeben wird, dann wird die Update-Quelle aus den Einstellungen für die Updateaufgabe der Antiviren-Datenbanken und Anwendungsmodule übernommen.

/W[A][!]:Protokolldatei • **/W:Protokolldatei** • **/WA:Protokolldatei**	Protokollieren von Ereignissen in der angegebenen Protokolldatei: • nur wichtige Ereignisse • alle Ereignisse Das Zeichen **!** bedeutet, dass die Protokolldatei nach jedem Aufgabenstart überschrieben wird. Die Angabe des absoluten oder relativen Dateipfads ist zulässig. Der Pfad wird in Anführungszeichen gesetzt, wenn er ein Leerzeichen enthält.
/APP	Update der Anwendungsmodule.

Beispiele:

```
KAVSHELL UPDATE ftp://ftp.kaspersky.ru/
/WA:avbases_upd.txt
KAVSHELL UPDATE /APP
```

9.4. Rollback des letzten Updates

Befehlssyntax:

```
KAVSHELL ROLLBACK [/W[A][!]:Protokolldatei]
```

Wenn keiner der Schlüssel angegeben wird, erscheinen Hilfeinformationen zur Befehlssyntax.

Schlüssel	Funktion
/W[A][!]:Protokolldatei • **/W:Protokolldatei** • **/WA:Protokolldatei**	Protokollieren von Ereignissen in der angegebenen Protokolldatei: • nur wichtige Ereignisse • alle Ereignisse Das Zeichen **!** bedeutet, dass die Protokolldatei nach jedem Aufgabenstart überschrieben wird. Die Angabe des absoluten oder relativen Dateipfads ist zulässig. Der Pfad wird in Anführungszeichen gesetzt, wenn er ein Leerzeichen enthält.

Beispiele:

```
KAVSHELL ROLLBACK /WA:rollback.log
```

9.5. Echtzeitschutzmodus

Befehlssyntax:

KAVSHELL RTP [taskid] { /START /PWD:password | /STOP /PWD:password }

Wenn keiner der Schlüssel angegeben wird, erscheinen Hilfeinformationen zur Befehlssyntax.

Schlüssel	Funktion
/START	Aktiviert den Echtzeitschutz oder eine bestimmte Echtzeitschutz-Komponente.
/STOP	Deaktiviert den Echtzeitschutz oder eine bestimmte Echtzeitschutz-Komponente.
taskid	Aufgaben-ID des Echtzeitschutzes. Wenn kein Identifikator (taskid) angegeben wird, werden alle Befehle auf alle Echtzeitschutz-Aufgaben angewandt. Mögliche Werte: • on-access – Echtzeitschutz für Dateien • mail-checker– Echtzeitschutz für E-Mails • outlook-plugin – Echtzeitschutz für Microsoft Office Outlook-E-Mails • script-checker – Skriptuntersuchung in Echtzeit • office-guard – Untersuchung von VBA-Makros
/PWD:password	Angabe des Administratorkennworts, das für die Ausführung des Befehls erforderlich ist.

Beispiele:

```
KAVSHELL RTP /START /PWD:password
KAVSHELL RTP on-access /START /PWD:password
KAVSHELL RTP /STOP script-checker /PWD:password
```

9.6. Start der Anwendung

Befehlssyntax:

```
KAVSHELL START
```

9.7. Beenden der Anwendung

Befehlssyntax:

```
KAVSHELL STOP /PWD:password
```

Schlüssel	Funktion
/PWD:password	Angabe des Administratorkennworts, das für die Ausführung des Befehls erforderlich ist.

Beispiel:

KAVSHELL STOP /PWD:password

9.8. Steuerung von Aufgaben

Befehlssyntax:

```
KAVSHELL TASK [ taskid {/START  [/W[A][!]:Protokolldatei]|
                       /STOP |
                       /PAUSE |
                       /RESUME [/W[A][!][: Protokoll-
datei]]|
                       /DELETE } ] /PWD:password
```

Wenn keiner der Schlüssel angegeben wird, wird eine Liste aller verfügbaren Aufgaben angezeigt, die ihre unikalen IDs und den Status jeder Aufgabe enthält.

Schlüssel	Funktion
/START	Start der Aufgabe mit dem angegebenen ID.

/W[A][!]:Protokolldatei • **/W:Protokolldatei** • **/WA:Protokolldatei**	Protokollieren von Ereignissen in der angegebenen Protokolldatei: nur wichtige Ereignisse alle Ereignisse Das Zeichen **!** bedeutet, dass die Protokolldatei nach jedem Aufgabenstart überschrieben wird. Die Angabe des absoluten oder relativen Dateipfads ist zulässig. Der Pfad wird in Anführungszeichen gesetzt, wenn er ein Leerzeichen enthält.
/STOP	Die Ausführung der Aufgabe mit dem angegebenen ID wird beendet. Für das Beenden von Echtzeitschutzaufgaben ist das Kennwort ein obligatorischer Parameter! Zu diesen Aufgaben gehören: • Echtzeitschutz für Dateien • Mail-Echtzeitschutz • Echtzeit-Untersuchung von Skripts • Untersuchung von VBA-Makros • Schutz vor Netzwerkangriffen
/PAUSE	Die Ausführung der Aufgabe mit dem angegebenen ID wird angehalten.
/RESUME	Die Ausführung der Aufgabe mit dem angegebenen ID wird fortgesetzt.
/DELETE	Löscht die Aufgabe mit dem angegebenen ID.
taskid	Unikaler Aufgaben-ID. Systemaufgaben können nach folgenden Standard-IDs gesteuert werden: • scan-computer – vollständige Untersuchung des Computers • scan-removable – Untersuchung von

	Wechsellaufwerken • scan-quarantine – Untersuchung der Quarantäne • scan-critical – Untersuchung der Laufwerksbootsektoren, des Arbeitsspeichers und der Autostart-Objekte • update-bases – Update der Antiviren-Datenbanken • update-app – Update der Anwendungsmodule • rollback – Rückgängigmachen des letzten Updates der Antiviren-Datenbanken • on-access – Echtzeitschutz für Dateien • mail-checker – Echtzeitschutz für E-Mail • script-checker – Skriptuntersuchung in Echtzeit • office-guard – Untersuchung von VBA-Makros • ids – Schutz vor Netzwerkangriffen
/PWD:password	Angabe des Administratorkennworts, das für die Ausführung des Befehls erforderlich ist.

Beispiele:

```
KAVSHELL TASK
KAVSHELL TASK update-app /START /WA:fullscan.log
/PWD:password
KAVSHELL TASK _LOCAL_0630cddf-0793-4c2d-be1e-a3daed0904c6
/DELETE /PWD:password
```

9.9. Import/ Export von Einstellungen

Befehlssyntax:

```
KAVSHELL IMPORT Konfigurationsdatei /PWD:password
KAVSHELL EXPORT Konfigurationsdatei /PWD:password
```

Schlüssel	Funktion
Konfigurations-datei	Name der Profildatei, aus der die Einstellungen für Kaspersky Anti-Virus importiert oder in die sie exportiert werden. Details über Profile s. Pkt. 5.10.3 auf S. 124.
/PWD:password	Angabe des Administratorkennworts, das für die Ausführung des Befehls erforderlich ist.

Beispiele:

```
KAVSHELL IMPORT c:\kav50settings.xml /PWD:password
KAVSHELL EXPORT c:\kav50settings.xml /PWD:password
```

9.10. Hinzufügen eines Lizenzschlüssels

Befehlssyntax:

```
KAVSHELL ADDKEY Datei [/R] /PWD:password
```

Schlüssel	Funktion
Datei	Name der Lizenzschlüsseldatei
[/R]	Ersetzen des aktiven Lizenzschlüssels durch einen neuen Lizenzschlüssel
/PWD:password	Angabe des Administratorkennworts, das für die Ausführung des Befehls erforderlich ist.

Beispiel:

```
KAVSHELL ADDKEY c:\00A531D2.key /R /PWD:password
```

KAPITEL 10. HÄUFIGE FRAGEN

In diesem Kapitel behandeln wir die von Benutzern am häufigsten gestellten Fragen zu Installation, Einstellung und Arbeit mit Kaspersky Anti-Virus und versuchen, sie eingehend zu beantworten.

Frage: Kann Kaspersky Anti-Virus mit Antiviren-Software von anderen Herstellern genutzt werden?

Um Konflikten aus dem Weg zu gehen, empfehlen wir, Antiviren-Software von anderen Herstellern vor Installation von Kaspersky Anti-Virus zu deinstallieren.

Frage: Kaspersky Anti-Virus untersucht eine Datei nicht zweimal. Warum?

In der Tat untersucht Kaspersky Anti-Virus eine Datei nicht doppelt, wenn sie seit der letzten Untersuchung nicht geändert worden ist.

Möglich geworden ist dieses Verhalten dank der neuen Technik von iChecker und iStreams. Dabei werden für Objekte Datenbanken mit Kontrollsummen verwendet und die Kontrollsummen von Dateien in zusätzlichen NTFS-Streams gespeichert.

Frage: Warum wird beim Einsatz von Kaspersky Anti-Virus die Leistung des Rechners gesenkt und der Prozessor erheblich belastet?

Die Untersuchung auf Viren ist eine rechnerische (mathematische) Aufgabe, die Strukturanalyse, Kontrollsummenberechnung und mathematische Neuberechnung der Daten beinhaltet. Daher ist die Prozessorzeit die Hauptressource, die von Kaspersky Anti-Virus während der Arbeit gebraucht wird. Dabei wird durch Hinzufügung eines jeden neuen Virus in die Antiviren-Datenbank die Gesamtzeit der Untersuchung verlängert.

Im Unterschied zu anderen Anti-Virus-Herstellern, die Untersuchungszeit durch Ausschluss von schwer zu identifizierenden oder (z. B. in der geographischen Region) seltener auftretender Viren bzw. schwierig zu analysierenden Dateiformate (z. B. pdf) verkürzen, vertritt Kaspersky Lab die Meinung, dass die Aufgabe von Kaspersky Anti-Virus darin besteht, einen realen Antivirenschutz für Benutzer zu bieten.

Für einen erfahrenen Benutzer beschleunigt Kaspersky Anti-Virus die Untersuchungszeit, weil einzelne Dateitypen von der Untersuchung ausgenommen werden. Es sollte jedoch nicht vergessen werden, dass die Sicherheit so geringer wird.

Kaspersky Anti-Virus erkennt über 1200 Formate archivierter und komprimierter Dateien und kann sechs Formate desinfizieren. Das ist für die Antiviren-Sicherheit sehr wichtig, weil jedes erkennbare Format einen ausführbaren schädlichen Code enthalten kann. Trotzdem arbeitet die neue Software schneller als der Vorgänger, obwohl sich die Gesamtzahl der von Kaspersky Anti-Virus erkannten Viren jeden Tag vergrößert, und die Anzahl erkennbarer Formate ansteigt. Erreicht wird dieses Tempo mit der einmaligen Technik iChecker™ und iStreams™, die Kaspersky Lab entwickelt hat.

Frage: Wozu wird der Lizenzschlüssel gebraucht? Kann mein Kaspersky Anti-Virus auch ohne ihn funktionieren?

Ohne Lizenzschlüssel kann Kaspersky Anti-Virus nicht laufen.

Wenn Sie sich noch nicht für den Kauf von Kaspersky Anti-Virus entschieden haben, können Sie von der Kaspersky-Lab-Webseite im Abschnitt **Download → Testversionen** eine Testversion des Programms herunterladen. Die Testversion funktioniert für 15 Tage. Nach Ablauf dieser Frist wird der Schlüssel gesperrt.

Frage: Was passiert, wenn die Lizenz für Softwarebenutzung abläuft?

Nach dem Ablauf der Lizenz für Kaspersky Anti-Virus bleibt die Software weiterhin funktionsfähig, Sie werden aber die Antiviren-Datenbanken nicht aktualisieren können. Es können nach wie vor infizierte Objekte mit Kaspersky Anti-Virus gesäubert werden, aber nur mit Zugriff auf alte Antiviren-Datenbanken.

Sollte eine solche Situation auftreten, informieren Sie Ihren Systemadministrator und wenden Sie sich an Ihren Händler, bei dem Sie Kaspersky Anti-Virus erworben haben bzw. direkt an Kaspersky Lab, um die Lizenz zu verlängern.

Frage: Wozu werden tägliche Updates gebraucht?

Noch vor einigen Jahren wurden Viren auf Disketten weiter gegeben und für den Schutz eines Computers genügte, ein Antiviren-Programm zu installieren und ab und zu die Antiviren-Datenbanken zu

aktualisieren. Die letzten Virenepidemien haben sich weltweit in wenigen Stunden verbreitet und ein installierter Kaspersky Anti-Virus mit alten Datenbanken ist hilflos bei der neuen Bedrohung. Um solchen neuen Viren nicht zum Opfer zu fallen, müssen die Antiviren-Datenbanken täglich aktualisiert werden.

Kaspersky Lab beschleunigt jedes Jahr die Frequenz für das Update der Antiviren-Datenbanken. Zurzeit werden sie stündlich aktualisiert.

Eine Zusatzfunktion ist die Aufgabe Update der Programmmodule von Kaspersky Anti-Virus, mit der erkannte Störungen korrigiert oder neue Funktionen zur Verfügung gestellt werden.

Frage: Was wurde im Updatedienst in der Version 5.0 geändert?

Für die Produktlinie der Version 5.0 hat Kaspersky Lab ein neues Service-Update eingerichtet. Die Entwicklung erfolgt auf Wunsch von Benutzern und Marketing-Fachleuten. Außerdem lautete die Aufgabe, den Update-Vorgang – angefangen bei der Vorbereitung durch Kaspersky Lab bis zum Update von Dateien bei den Benutzern.

Vorteil des Update-Services:

- Wiederaufnahme des Downloads von Dateien nach Verbindungsabbruch. *Jetzt müssen bereits empfangene Updates nach Wiederherstellung der Verbindung nicht noch einmal geladen werden.*
- Zweifache Verkleinerung bei der Größe des kumulativen Updates. Das kumulative Update enthält die gesamte Antiviren-Datenbank, deshalb ist das Kumulativum erheblich größer als ein gewöhnliches Update. Im neuen Service kommt eine spezielle Technik zum Einsatz, mit der bereits vorhandene kumulative Updates genutzt werden können.
- Schnellerer Download aus dem Internet. Kaspersky Anti-Virus sucht den Update-Server von Kaspersky Lab aus, der in Ihrer Region liegt. Außerdem wird die Belastung des Servers je nach dessen Performance geprüft, Sie gelangen also nicht auf einen überlasteten Server, wenn ein anderer Server ausfällt.
- „Schwarze Liste“ mit Lizenzschlüsseln. Mit dieser Liste können Benutzer vom Update abgehalten werden, die keine Lizenz für Kaspersky Anti-Virus haben. Dadurch leiden lizenzierte Benutzer nicht unter überlasteten Update-Servern.
- Bei den Corporate-Produkten können noch lokale Update-Server angelegt werden. Diese Funktion wird bei den

Organisationen gebraucht, wo in einem lokalen Netz Computer verknüpft sind, die von Kaspersky-Lab-Programmen geschützt werden. In so einem Fall kann jeder Computer als Update-Server konfiguriert werden, der Updates aus dem Internet lädt, sie in ein lokales Verzeichnis verschiebt und den anderen Netzcomputern den Zugriff ermöglicht.

Frage: Kann ein Übeltäter Antiviren-Datenbanken ersetzen?

Alle Antiviren-Datenbanken haben eine eigenartige Signatur, die beim Zugriff auf die Datenbanken von Kaspersky Anti-Virus überprüft wird. Entspricht die Signatur nicht der durch Kaspersky Lab zugeordneten Signatur, und hat die Datenbank ein späteres Datum, als das Lizenzablaufdatum, so wird Kaspersky Anti-Virus solche Datenbanken nicht verwenden.

Frage: Wie kann das Update eines Rechners aus dem Internet und das nachfolgende Update für die anderen Netzcomputer eingerichtet werden?

Wir bezeichnen als Server den Computer, der sich sein Update aus dem Internet holt und die anderen Rechner sind Clients für diesen Server.

Es gibt mehrere Möglichkeiten, um Updates aus dem lokalen Netz zu empfangen:

- Lokale Update-Quelle auf dem Server von Kaspersky Administration Kit 5.0 aktivieren.

  Kaspersky Administration Kit hat eingebaute Mittel für die Update-Weiterleitung in einem Corporate Net. Der Kit kann nach einem festgelegten Zeitplan die Ressource mit allgemeinem Zugriff aktualisieren und Update-Aufgaben auf den restlichen Computern starten. Kaspersky Administration Kit passt auf, dass die Menge der aus dem Internet zu ladenden Daten nicht die Bedürfnisse der installierten Programme übertrifft. Auf dem Server liegt eine Liste mit den verfügbaren Patches zur Ansicht bereit. Näheres zum Einstellungsvorgang finden Sie im Handbuch für den Systemadministrator von „Kaspersky Administration Kit 5.0“.

- Lokale Update-Quelle in einem Produkt von Kaspersky Lab aktivieren.

  Diese Variante muss genutzt werden, wenn der Kaspersky

Administration Kit nicht verwendet werden kann oder wenn eine komplizierte Netzstruktur für die Update-Server vorhanden ist. Es muss Folgendes getan werden:

- Es müssen die Rechner bestimmt werden, die als Update-Server dienen werden. Auf diesen Computern werden die Programme von Kaspersky Lab mit der Version 5.0 installiert[8].
- Auf jedem gewählten Computer muss eine Netzressource angelegt werden, die als Update-Weiterleitung dient. Das kann ein Netzordner auf einem Microsoft Windows-Rechner, ein ftp- oder ein http-Server sein. Die Zugriffsrechte für diesen Ordner müssen ordnungsgemäß zugewiesen sein.
- Es muss eine Update-Aufgabe angelegt oder eine vorhandene Aufgabe geändert werden. Die Heranziehung des Updates aus der lokalen Quelle muss aktiviert sein und auf den angelegten Ordner verwiesen werden.
- Auf allen Computern, die von diesem Server aktualisiert werden sollen, muss als Quelle die lokale Update-Quelle des Servers angegeben werden.

Frage: Ich verwende einen Proxy-Server und das Update funktioniert nicht. Was muss ich machen?

Probleme beim Update-Download unter Einsatz eines Proxyservers können folgende Ursachen haben:

- Die Netzwerkeinstellungen sind nicht korrekt.

  Beim Einstellen des Update-Service gibt es zwei Methoden zum Anpassen für die Netzeinstellungen: Übernahme der Einstellungen von Microsoft Internet Explorer oder eigene Einstellungen übernehmen. Der Update-Service übernimmt die Einstellungen aus Microsoft Internet Explorer nicht immer korrekt. Folgende Fälle sind bekannt:

  - Der Rechnung ist nicht für das Internet eingestellt.
  - Die Einstellungen im Microsoft Internet Explorer lassen sich nicht ändern, wenn kein Benutzer angemeldet ist.
  - Der Proxy-Server verlangt eine Autorisierung.

[8] außer Kaspersky Anti-Virus 5.0 Personal und Kaspersky Anti-Virus 5.0 for Microsoft ISA Server

In solchen Fällen müssen die Netzwerkeinstellungen unmittelbar in den Einstellungen für den Update-Service eingegeben werden.

- Verwendung eines Proxy-Servers, der vom Typ her nicht vom Update-Service des Kaspersky Anti-Virus unterstützt wird.

  Der Update-Service arbeitet nicht mit Kerio WinRoute zusammen, da WinRoute nicht vollständig das Protokoll http 1.0 realisiert. In diesem Fall empfehlen wir, einen beliebigen anderen Proxy-Server zu verwenden.

  Der Update-Service funktioniert auch nicht mit dem ftp-Protokoll über den Microsoft ISA Server. In diesem Fall empfehlen wir, die Updates von den Servern bei Kaspersky Lab über das http-Protokoll abzuwickeln.

Frage: Nach der Installation von Kaspersky Anti-Virus ist die Verbindung mit dem lokalen Netzwerk/Internet verloren gegangen. Was tun?

Es deutet darauf hin, dass ein Konflikt zwischen dem Modul von Kaspersky Anti-Virus, das dem Schutz vor Netzwerkangriffen dient, und einer auf Ihrem Computer installierten Firewall aufgetreten ist.

Um die Verbindung mit dem lokalen Netzwerk/Internet wiederherzustellen, schalten Sie den Schutz vor Netzwerkangriffen ab. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Hauptfenster von Kaspersky Anti-Virus und gehen Sie auf die Registerkarte **Einstellungen** (s. Abbildung 3).
2. Öffnen Sie mit dem Hyperlink Echtzeitschutz das Fenster **Echtzeitschutz-Einstellungen** und gehen Sie auf die Registerkarte **Netzwerk** (s. Abbildung 24).
3. Deaktivieren Sie das Kontrollkästchen **Echtzeitschutz vor Netzwerkangriffen aktivieren** und klicken Sie auf die Schaltfläche **OK**.

Damit die von Ihnen vorgenommenen Einstellungen wirksam werden, ist der Neustart des Computers erforderlich. Klicken Sie dazu im Fenster mit der entsprechenden Anfrage auf die Schaltfläche **Ja**. Wenn Sie den Computer später neu starten möchten, klicken Sie auf **Nein**.

Frage: Nach der Installation von Kaspersky Anti-Virus verhält sich das Betriebssystem ungewöhnlich ("Einfrieren auf blauem Bildschirm", wiederholter Neustart des Computers u.a.). Was tun?

Das bedeutet, dass ein Konflikt bei der gleichzeitigen Arbeit von Kaspersky Anti-Virus und einem bestimmten Programm aufgetreten ist.

Gehen Sie folgendermaßen vor, um die Funktionsfähigkeit Ihres Betriebssystems wiederherzustellen:

1. Klicken Sie gleich nachdem der Computer gestartet wurde solange auf die Taste **F8**, bis das Auswahlmenü für die Startvarianten des Betriebssystems erscheint.
2. Wählen Sie den Punkt **Abgesicherter Modus** und laden Sie das Betriebssystem.
3. Starten Sie Kaspersky Anti-Virus.
4. Gehen Sie im Programmhauptfenster auf die Registerkarte **Einstellungen** und klicken Sie auf den Hyperlink Erweiterte Einstellungen.
5. Wechseln Sie im folgenden Fenster **Erweiterte Einstellungen** auf die Registerkarte **Sicherheit** (s. Abbildung 61) und deaktivieren Sie das Kontrollkästchen **Kaspersky Anti-Virus bei Systemstart starten**. Klicken Sie auf **OK**.
6. Starten Sie das Betriebssystem im gewöhnlichen Modus neu.

Wenden Sie sich danach über die Kaspersky-Lab-Webseite an den Technischen Support-Service (Abschnitt **Dienste → Technischer Support → Anfrage an den Support senden**). Beschreiben Sie das Problem und die entsprechenden Bedingungen möglichst genau.

Fügen Sie Ihrer Anfrage unbedingt eine Datei mit dem vollständigen Speicherabbild des Betriebssystem Microsoft Windows bei. Diese Datei wird folgendermaßen erstellt:

1. Klicken Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz** und wählen Sie im folgenden Fenster den Punkt **Eigenschaften**.
2. Wählen Sie im folgenden Fenster **Systemeigenschaften** die Registerkarte **Erweitert** und klicken Sie im Abschnitt **Starten und Wiederherstellen** auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im Fenster **Starten und Wiederherstellen** im Abschnitt **Debuginformationen speichern** aus der Dropdown-Liste den Wert **Vollständiges Speicherabbild**.

   Die Datei mit dem Speicherabbild wird standardmäßig unter dem Namen *memory.dmp* im Systemordner gespeichert. Sie können einen anderen Ordner zum Speichern des Dumps festlegen. Ändern Sie dazu im entsprechenden Feld den Ordnernamen.
4. Wiederholen Sie den Vorgang, bei dem das mit der Arbeit von Kaspersky Anti-Virus verbundene Problem aufgetreten ist.
5. Vergewissern Sie sich, dass die Datei mit dem vollständigen Speicherabbild erfolgreich gespeichert wurde.

ANHANG A. KONTAKT ZUM TECHNISCHEN KUNDENDIENST

Kaspersky Anti-Virus bietet Ihnen die Möglichkeit, in folgenden Fällen Kontakt mit dem Technischen Support-Service aufzunehmen:

- Das Programm scheint nicht wie gewöhnlich zu funktionieren und bei der Arbeit treten Störungen auf.
- Kaspersky Anti-Virus hat ein Objekt gefunden, das möglicherweise von einem Virus oder dessen Modifikation infiziert ist, und das Objekt gesperrt. In dem Objekt befinden sich für Sie sehr wichtige Informationen und Sie möchten weiter mit der Datei arbeiten.

Wenn bei der Verwendung von Kaspersky Anti-Virus Probleme auftreten, vergewissern Sie sich zuerst, ob die vorliegende Dokumentation (insbesondere der Abschnitt **Häufige Fragen** (s. Kapitel 10 auf S. 211) oder der Abschnitt **Dienste/Wissensdatenbank** auf der Kaspersky-Lab-Webseite (www.kaspersky.com/de) keine Lösungsmethode für Ihr Problem enthält.

Wenn Sie in der Dokumentation und in der Wissensdatenbank auf der Webseite keine Lösung finden können, empfehlen wir Ihnen, sich an den Technischen Support-Service von Kaspersky Lab zu wenden.

Zur Lösung dringender Probleme können Sie die Servicenummer anrufen, die in Anhang C.2 auf S. 239genannt wird. Die telefonische technische Unterstützung wird rund um die Uhr auf Russisch, Englisch, Französisch und Deutsch angeboten. Bitte beachten Sie, dass Sie den Status eines registrierten Benutzers besitzen müssen, um den technischen Support in Anspruch zu nehmen. Außerdem benötigt der Servicemitarbeiter Ihre Registrierungsnummer (bei Erwerb einer verpackten Produktvariante) oder Ihre Bestellungsdaten (bei Erwerb des Produkts über das Internet).

Um eine Nachricht über Funktionsstörungen des Programms an den Technischen Support-Service zu senden,

verwenden Sie den Hyperlink Anfrage an den Technischen Kundendienst im linken Teil der Registerkarte **Support** (s. Abbildung 4) des Programmhauptfensters.

Es wird automatisch die Webseite von Kaspersky Lab geöffnet, auf der sich ein Formular für eine Anfrage an den Technischen Support-Service befindet. Füllen

Sie das Formular aus. Im ersten Fenster des Formulars sind Angaben über das aufgetretene Problem und die Lizenz für Kaspersky Anti-Virus erforderlich:

- Wählen Sie den **Typ der Anfrage**, indem Sie aus der Dropdown-Liste das Problem auswählen, das bei der Arbeit mit Kaspersky Anti-Virus aufgetreten ist.
- Wählen Sie **Kaspersky Anti-Virus for Windows Workstations** als Name des Kaspersky-Lab-Produkts und beschreiben Sie das Problem im Feld **Bitte beschreiben Sie Ihre Anfrage** ausführlich.
- Wählen Sie den Registrierungstyp des Programms: Wählen Sie **Lizenzschlüssel**, wenn Sie das Produkt als verpackte Variante gekauft und den Lizenzschlüssel von einer Diskette installiert haben, oder **Online Store Bestellnummer**, wenn Sie das Programm in einem Internet-Shop erworben haben.
- Geben Sie im Feld **Serien- oder Bestellnummer** die Seriennummer an. Diese Informationen finden Sie im Fenster **Verwaltung der Lizenzschlüssel** (s. Abbildung 106) im Feld **Nummer**.
- Geben Sie im Feld **Email** Ihre E-Mail-Adresse an.
- Klicken Sie auf die Schaltfläche **Next**.

Im nächsten Fenster des Formulars sind Informationen über das auf Ihrem Computer installierte System, Software, Hardware und Peripheriegeräte erforderlich. Sie können die Angaben manuell in die entsprechenden Formularfelder eintragen oder einen speziellen Dienst zum automatischen Sammeln dieser Informationen verwenden. Stellen Sie in diesem Fall sicher, dass der Start von ActiveX-Objekten erlaubt ist und klicken Sie auf die Schaltfläche **Find automatically**. Geben Sie außerdem folgende Informationen an:

- Wenn bei der Arbeit mit Kaspersky Anti-Virus for Windows Workstations ein Kompatibilitätsproblem mit einem anderen Programm aufgetreten ist, nennen Sie den Namen des Programms bitte im Abschnitt **Incompatibility Detected**.
- Geben Sie Ihre Informationen im Abschnitt **Kontaktinformationen** an, damit wir Ihnen antworten und das Problem möglichst schnell lösen können.
- Geben Sie den speziellen Zahlencode, der im Abschnitt **Automatic registration protection** angezeigt wird, in dem daneben liegenden Feld ein und klicken Sie auf die Schaltfläche **Submit**.

Wenn Kaspersky Anti-Virus eine möglicherweise infizierte Datei unter Quarantäne gestellt hat, können Sie die Antiviren-Datenbanken aktualisieren und die Desinfektion des Objekts versuchen (Details s. Pkt. 5.10.1.2 auf S. 114). Sollte

die Desinfektion des Objekts nicht möglich sein, Sie möchten das Objekt aber möglichst schnell wiederherstellen, dann können Sie das Objekt zur Analyse an Kaspersky Lab senden. Möglicherweise ist das Objekt tatsächlich von einer neuen, bisher noch unbekannten Virusart infiziert oder ein Fehlalarm ist eingetreten.

Achtung! Sie können von Ihnen verdächtigte Dateien nur dann an Kaspersky Lab senden, wenn sie mit Datenbanken untersucht worden sind, die am Absendetag aktualisiert wurden.

Um eine verdächtige Datei zur Analyse an Kaspersky Lab zu senden,

wählen Sie die Datei im Fenster **Quarantäne** (Details s. Pkt. 5.10.1.2 auf S. 114) aus und klicken Sie auf **Senden**.

Automatisch wird das Fenster des auf Ihrem Computer standardmäßig verwendeten Mailprogramms geöffnet (z.B. Microsoft Outlook Express), in dem eine E-Mail-Nachricht erstellt wird, an welche die möglicherweise infizierte Datei angehängt wird. Senden Sie die E-Mail ab. Die Kaspersky-Lab-Experten werden die eingesandte Datei sorgfältig prüfen und die Wiederherstellung aller darin enthaltenen Daten versuchen. Auf jeden Fall werden Sie eine ausführliche Antwort mit den Analyseergebnissen der Datei erhalten.

Bitte beachten Sie, dass jede Datei (höchstens 3 Dateien für einen Tag), die Sie an Kaspersky Lab senden möchten, mindestens 3 Tage vor dem Absenden mit Kaspersky Anti-Virus untersucht worden sein muss.

Es kann vorkommen, dass Kaspersky Anti-Virus bei der Untersuchung eine möglicherweise infizierte Datei nicht erkannt hat, Sie aber vollkommen sicher sind, dass eine oder mehrere Dateien Ihres Computers von einem neuen Virustyp infiziert sind. Auch solche Dateien können zur Analyse an Kaspersky Lab geschickt werden

Um Dateien, die Sie für infiziert halten, zur Analyse an Kaspersky Lab zu senden,

verwenden Sie den Hyperlink Einschicken einer Datei zur Untersuchung im linken Teil der Registerkarte **Support** (s. Abbildung 4). Geben Sie im Standardfenster zur Dateiauswahl die Dateien an, die Sie für verdächtig halten.

Das Vorgehen zum Senden einer E-Mail-Nachricht an Kaspersky Lab ist absolut identisch mit dem Vorgehen, das für möglicherweise infizierte Objekte, die aus Quarantäne abgesandt werden, beschrieben wurde.

ANHANG B. GLOSSAR

In den vorliegenden Unterlagen treten spezifische Termini und Begriffe aus dem Bereich Virenschutz auf. Glossar stellt eine Erläuterung dieser Begriffe dar. Um die Benutzung des Glossars zu erleichtern, haben wir die Begriffe alphabetisch angeordnet.

A

Administrierungsagent – spezielle Anwendung für das Zusammenwirken des Administrierungsservers mit **Programmen**, die zu den Produkten von Kaspersky Lab gehören. Dazu zählt der Kaspersky Administration Kit 5.0.

Administrator (Sicherheit) – Person, die das Antivirus-Programm bedient. Sie kann im Remote-Betrieb mit der *Administrierungskonsole* oder mithilfe der lokalen Schnittstelle arbeiten.

Administrator des logischen Netzes – eine Person, die Kaspersky Anti-Virus über das zentrale Fernverwaltungssystem Kaspersky Administration Kit 5.0 verwaltet.

Administrierungskonsole – eine Komponente, die eine grafische Oberfläche für die Verwaltung von Kaspersky Anti-Virus bietet. Sie gehört zum Kaspersky Administration Kit 5.0.

Administrierungsserver – Spezialsoftware, mit den Funktionen zentraler Ablage von Informationen über die im Netzwerk installierten Anwendungen des Kaspersky Lab und die Verwaltung von diesen. Verwaltungsagent gehört zum Lieferumfang von Kaspersky Administration Kit 5.0.

Aktiver Lizenzschlüssel – für den Betrieb des Kaspersky Anti-Virus installierte und für den Betreib von Kaspersky Anti-Virus im laufenden Zeitraum eingesetzte Lizenzschlüssel. Dieser bestimmt die Lizenzdauer und die Software betreffende Lizenzpolitik. Das Programm kann nur einen aktiven Schlüssel besitzen.

Aktualisierung – Ersetzen/Ergänzen von neuen Dateien (Antiviren-Datenbanken oder Programmmodule) über die Update-Server von Kaspersky Lab.

Anfällige Dateien nach Erweiterung untersuchen - bei Datei-Untersuchung wird die Erweiterung des Dateinamens berücksichtigt.

Anfällige Dateien nach Format untersuchen - bei der Untersuchung wird der interne Datei-Inhalt, und zwar das Formatkennzeichen im Dateikopf analysiert.

Antiviren-Datenbanken – von Spezialisten des Kaspersky Lab erstellte Datenbanken, welche eine detaillierte Beschreibung aller derzeit bekannten Viren und deren Behandlungsmethoden enthalten. Die

Datenbanken werden bei Kaspersky Lab mit Auftreten neuer Viren ständig aktualisiert. Um die Genauigkeit der Virenerkennung zu erhöhen, empfehlen wir, die Updates für Antiviren-Datenbanken regelmäßig zu kopieren.

Aufgabe – Aktion, die von einer von Kaspersky Lab entwickelten Anwendung ausgeführt wird.

Ausschlüsse – eine Reihe von Einstellungen, mit denen die Untersuchung verschiedener Objekte abgeschaltet wird. Sie können Ihre eigenen Ausschlüsse für den Echtzeitschutz und der vollständigen Untersuchung festlegen. So können Sie z.B. die Untersuchung der Archive während der vollständigen Untersuchung abschalten oder bestimmte Dateimasken angeben, die Sie nicht untersuchen möchten.

Autostartup-Objekte – Programme, die für den Start und korrekten Betrieb des/der auf Ihrem Computer installierten Betriebssystems/Software notwendig sind. Bei jedem Systemstart werden gleichzeitig diese Objekte gestartet. Es gibt Viren, die eben solche Objekte befallen können, wodurch z.B. der Systemstart gesperrt werden kann.

B

Backup – spezielle Ablage, in der Sicherheitskopien von Objekten gespeichert bleiben, bevor diese gesäubert oder gelöscht werden.

Backup-Kopie – Erstellung einer Sicherungskopie für eine Datei, bevor diese gesäubert oder gelöscht wird. Diese Kopie wird in der Backup-Ablage gespeichert und kann zur späteren Wiederherstellung der Datei, z.B. zwecks deren Untersuchung mit aktualisierten Antiviren-Datenbanken dienen.

D

Dateimaske – aus allgemeinen Zeichen bestehender Platzhalter für den Namen und die Namenserweiterung einer Datei. Die beiden wichtigsten Zeichen für Dateimasken sind * und ? (* kann für eine beliebige Anzahl von Zeichen stehen, ? für ein einzelnes Zeichen). Mit Hilfe dieser Zeichen lässt sich jeder beliebige Dateinamen darstellen. Beachten Sie, dass Name und Namenserweitung einer Datei stets durch einen Punkt getrennt werden.

Dringende Updates – kritische Updates für Anwendungsmodule.

E

Echtzeitschutz – ein Betriebsmodus, in dem sich die Anwendung ständig im Arbeitsspeicher des Computers befindet und Zugriffe auf Objekte des Dateisystems überwacht werden. Bevor die Anwendung den Zugriff auf ein Objekt freigibt durchsucht sie dieses auf Viren. Wird ein Virus erkannt, so wird ein Säuberungsversuch unternommen. Anderenfalls wird das Objekt gelöscht oder (abhängig von den von Ihnen vorgenommenen Einstellungen) der Zugriff auf das Objekt gesperrt.

Einstellungsdatei – Datei, in der die Grundeinstellungen des Programms gespeichert sind. Die Einstellungen lassen sich in eine Datei exportieren (speichern) und aus einer Datei importieren (laden).

Empfohlen – Sicherheitsstufe, die auf den von den Experten des Kaspersky Lab empfohlenen Einstellungen basiert und einen optimalen Schutz für Ihren Rechner bietet. Diese Sicherheitsstufe gilt als Vorgabe.

Erweiterte Antiviren-Datenbanken – *Standard-Datenbanken* plus zusätzliche Datenbanken, welche es ermöglichen, potentiell gefährlicher Software auf Ihrem Computer zu entdecken.

G

Gefährliche Programme (*Riskware*) – Programmlösung, die keine schädliche Funktion ausübt, von böswilligen Benutzern jedoch als Hilfsmittel für schädliche Programme missbraucht werden können, da sie Bugs und Fehler enthalten. Zu dieser Gruppe gehören zum Beispiel Programme mit Remote-Steuerung, IRC-Clients, FTP-Server, viele Utilities zum Anhalten oder Verstecken von Prozessen.

Gruppenrichtlinie – Parametersatz für den Einsatz der Anwendung in der Verwaltungsgruppe, wenn diese über Kaspersky Administration Kit 5.0 verwaltet wird.

H

Hacker-Utilities (*Hack Tools*) – Programmlösung, die böswillige Nutzer zu eigenen Zielen missbrauchen, um in Ihren Computer einzudringen. Zu dieser Gruppe gehören verschiedene illegale Scanner, Programme für das Knacken von Passwörtern, weitere Programmabarten für den Einbruch in Netzressourcen oder für das Eindringen in ein angegriffenes System.

I

iChecker™ – ein Verfahren, mit dem die Objekte, die seit der letzten Untersuchung nicht geändert wurden, aus der Untersuchung ausgeschlossen werden können. Dieses Verfahren verwendet eine Datenbank mit Kontrollsummen der Objekte.

Infiziertes Objekt – ein Objekt, in dem ein schädlicher Code eingebettet ist. Wir empfehlen Ihnen nicht, mit solchen Objekten zu arbeiten, weil dadurch das Infektionsrisiko für Ihren Computer ansteigen kann.

iStreams™ – ein Verfahren, mit dem die Untersuchung von den auf einem Laufwerk mit dem NTFS-Dateisystem befindlichen Dateien, die seit der letzten Untersuchung nicht geändert wurden, ausgeschlossen werden kann. Dieses Verfahren verwendet die Ablage von Datei-Kontrollsummen in zusätzlichen NTFS-Streams.

K

Kaspersky Administration Kit 5.0 – eine Anwendung, die zum Lieferumfang von Kaspersky Business Optimal und Kaspersky Corporate Suite gehört und zur zentralen Verwaltung der wichtigsten

Administrationsaufgaben im Bereich Antiviren-Sicherheit für die auf der Basis von Anwendungen des Kaspersky Lab aufgebaute Unternehmensnetzwerke dient.

L

Lizenzdauer – ein Zeitraum, in dem Sie die vollständige Funktionalität des Kaspersky Anti-Virus nutzen können. Die Lizenzdauer wird durch den Lizenzschlüssel bestimmt und beträgt in der Regel ein Kalenderjahr ab Aktivierung des Lizenzschlüssels. Mit dem Lizenzablauf wird die Funktionalität der Software eingeschränkt: Sie werden die Antiviren-Datenbanken und die Programmmodule nicht mehr aktualisieren können.

Lizenzschlüssel - eine Datei mit Erweiterung *.key, die Ihren eigenen „Schlüssel" für die Arbeit mit Kaspersky Anti-Virus darstellt. Der Lizenzschlüssel gehört zum Lieferumfang der Software, sofern Sie diese bei Vertriebspartnern des Kaspersky Lab erworben haben, oder wird Ihnen per E-Mail zugesandt, sofern die Software im Online-Shop erworben wurde. Ohne Lizenzschlüssel kann Kaspersky Anti-Virus NICHT LAUFEN.

M

Mail-Datenbanken – Datenbanken, die auf Ihrem Rechner abgelegten E-Mail-Nachrichten beinhalten. Nach Eingang/Absendung wird jede eingegangene/abgesandte Nachricht in der Mail-Datenbank abgelegt. Solche Datenbanken werden im Laufe einer vollständigen Untersuchung des Computers durchsucht.

Maximale Sicherheit – Sicherheitsstufe, die den maximal möglichen Schutz für Ihren Rechner bei einigem Leistungsrückgang des Systems bietet.

Maximales Tempo – Sicherheitsstufe, bei der eine maximale Betriebsgeschwindigkeit gewährleistet und die Anzahl der zu untersuchenden Objekte eingeschränkt wird.

Module der Anwendung – Dateien, die zu der Distribution von Kaspersky Anti-Virus 5.0 für Windows Workstations gehören und zur Realisierung der Basisaufgaben des Produkts dienen. Jeder Typ der Aufgaben, die von Kaspersky Anti-Virus realisiert werden (*Echtzeitschutz*, *Scan auf Befehl*, *Update*) entspricht einem ausführbaren Modul. Durch den Start der vollständigen Untersuchung Ihres Computers aus dem Hauptfenster initiieren Sie den Start des Moduls dieser Aufgabe.

O

Objekt löschen – Behandlungsmöglichkeit für ein Objekt, bei der das Objekt vom Computer physisch entfernt wird. Es wird empfohlen, diese Behandlungsmöglichkeit für infizierte Objekte zu wählen. Stellt das Löschen eine primäre Aktion mit dem Objekt dar, so wird vor deren Ausführung für das Objekt eine Backup-Kopie angelegt. Sie können

diese Kopie zur Wiederherstellung des ursprünglichen Objekts verwenden.

Objektsäuberung beim Neustart – die effektivste Art der Behandlung von infizierten Objekten, die beim Säuberungsversuch von anderen Anwendungen genutzt werden. Dabei wird das infizierte Objekt kopiert und die erstellte Kopie gesäubert. Beim nächsten Neustart des infizierten ursprünglichen Objekts wird dieses durch seine gesäuberte Kopie ersetzt. In den Betriebssystemen Microsoft Windows 9x werden bei gesäuberten Objekten mit langen Namen deren Namen verkürzt. Daher können die auf die gesäuberten Objekte zugreifenden Anwendungen möglicherweise nicht korrekt laufen.

Objekt sperren – Zugriff auf das Objekt für externe Anwendungen sperren. Das gesperrte Objekt kann werden gelesen noch ausgeführt, geändert oder gelöscht werden.

OLE-Objekt – Objekte oder Dokumente, die in andere Dateien mittels OLE-Technologie eingebettet sind.

P

Plugin zur Verwaltung des Anwendungsbetriebs – eine spezielle Komponente, die eine Schnittstelle zur Fernverwaltung des Anwendungsbetriebs über die Administrierungskonsole zur Verfügung stellt. Jede Anwendung hat ihren eigenen Plugin. Plugins gehören zum Lieferumfang aller Anwendungen des Kaspersky Lab, die mittels Kaspersky Administration Kit 5.0 verwaltet werden können.

Potentiell gefährliche Programme sind Programme, die zwar keine Viren darstellen, aber eine potentielle Bedrohung enthalten. Unter bestimmten Umständen stellt das Vorhandensein solcher Programme auf dem Computer eine Gefahr für Ihre Daten dar. Zu dieser Kategorie zählen Dienstprogramme zur entfernten Administration, Dialer (Programme zur automatischen Einwahl auf kostenpflichtige Internetressourcen), die eine Telefonverbindung benutzen, und andere.

Q

Quarantäne – spezielle Datenablage zur Isolierung von infizierten und verdächtigen Objekten.

R

Reserveschlüssel – für den Betrieb des Kaspersky Anti-Virus installierte aber nicht aktivierte Lizenzschlüssel. Der Reserveschlüssel wird mit dem Ablauf des derzeit gültigen Lizenzschlüssels aktiviert.

S

Säuberung von Objekten – Behandlung von *infizierten Objekten*, nach welcher die Daten völlig oder teilweise wiederhergestellt werden oder die Entscheidung getroffen wird, dass die betreffenden Objekte nicht gesäubert werden können. Objekte werden auf der Basis von Einträgen in den Antiviren-Datenbanken gesäubert. Stellt Säuberung eine primäre

Aktion mit dem Objekt dar (die erste Aktion mit dem Objekt, gleich als dieses erkannt wurde), so wird vor deren Ausführung für das Objekt eine Backup-Kopie angelegt. Während der Säuberung können die Daten teilweise verloren gehen. Sie können diese Kopie zur Wiederherstellung des ursprünglichen Objektzustands (wie er vor dem Säuberungsversuch war) verwenden.

Scherzprogramme (*Jokes*) sind Software, die dem Computer keinen Schaden zufügen, sondern Meldungen darüber anzeigen, dass bereits Schaden verursacht wurde oder unter bestimmten Bedingungen Schaden angerichtet wird. Solche Programme warnen den Benutzer häufig vor fiktiven Bedrohungen. So kann beispielsweise eine Meldung angezeigt werden, die über das Formatieren der Festplatte informiert (obwohl dies nicht der Wirklichkeit entspricht) oder einen Virusfund in Dateien meldet, die aber tatsächlich virusfrei sind.

„Schwarze" Liste – Datenbank, die Informationen über Lizenzschlüssel, deren Besitzer die Bestimmungen der Lizenzvereinbarung nicht eingehalten haben, sowie über geschriebene aber aus irgendeinem Grund nicht verkaufte Schlüssel enthält. Die Inhalte der „schwarzen Liste" werden mit den Antiviren-Datenbanken täglich aktualisiert; ohne sie wird Kaspersky Anti-Virus nicht laufen.

(Sicherheits-) Administrator – eine Person, die Software verwaltet. Diese Person kann die Software sowohl über das Netzwerk von der Konsole oder dem Administrierungsserver als auch von der lokalen Schnittstelle verwalten.

Spyware – Programmlösung, deren Ziel der nicht sanktionierte Zugriff auf Benutzerdaten, das Erschleichen von Aktionen auf dem Computer, das Sammeln von Informationen über den Inhalt der Festplatte ist. Solche Programme erlauben böswilligen Benutzern nur das Sammeln von Informationen, nicht jedoch die Übernahme eines fremden Computers. Spionage-Programme verbreiten sich in der Regel mit kostenlosen Programmen und richten sich vom Benutzer unerkannt auf dem Rechner ein. Zu dieser Gruppe gehören Tastatur-Spione, Programme zum Knacken von Passwörtern, Sammelprogramme für vertrauliche Informationen (zum Beispiel Kreditkartennummern).

Status des Antiviren-Schutzes – aktueller Zustand des Antiviren-Schutzes, der den Sicherheitsgrad des Computers charakterisiert.

T

Tarnprogramme (*Rootkit*) sind Dienstprogramme, die der Tarnung von schädlicher Aktivität dienen. Sie maskieren schädliche Programme, um zu vermeiden, dass diese von Antivirenprogrammen gefunden werden. Rootkits sind außerdem fähig, das Betriebssystem des Computers zu modifizieren und dessen Grundfunktionen zu ersetzen, wodurch sie die eigene Existenz und Aktionen verbergen, die ein Angreifer auf dem infizierten Computer vornimmt.

U

Unbekanntes Virus – ein neues Virus, über welches es noch keine Informationen in den Antiviren-Datenbanken gibt. In der Regel erkennt Kaspersky Anti-Virus unbekannte Viren in Objekten mit Hilfe des *heuristischen Codeanalysators*. Die erkannten Objekte erhalten den Status *verdächtig*.

Update-Server des Kaspersky Lab – Auflistung von http- und ftp-Seiten Aktualisierung der des Kaspersky Lab, von denen Kaspersky Anti-Virus die Antiviren-Datenbanken und Programmmodule auf Ihren Rechner kopiert.

V

Verdächtiges Objekt – ein Objekt, dessen Code entweder einen modifizierten Code eines bekannten Virus oder einen virusähnlichen Code enthält, der Kaspersky Lab noch unbekannt ist.

Verfügbare Updates - Service Packs mit einem Satz von dringenden Updates, die in einem bestimmten Zeitraum gesammelt wurden bzw. Änderungen an der Anwendungsarchitektur.

Verschieben von Objekten in Quarantäne – Behandlungsmöglichkeit für ein verdächtiges Objekt. Dabei wird der Zugriff auf das betreffende Objekt gesperrt und das Objekt zur späteren Behandlung in die Quarantäne-Ablage verschoben.

Vertrauenswürdige Prozesse – Liste der Programmprozesse, deren Dateiaktivität im Echtzeitschutzmodus nicht von Kaspersky Anti-Virus kontrolliert wird. Alle von vertrauenswürdigen Prozessen gestarteten, geöffneten und gespeicherten Objekte, werden nicht untersucht.

Verwaltungsagent – Spezialsoftware, die Zusammenarbeit zwischen dem Administrierungsserver und den zur korporativen Software des Kaspersky Lab gehörenden Anwendungen ermöglicht. Verwaltungsagent gehört zum Lieferumfang von Kaspersky Administration Kit 5.0.

Verwaltungsgruppe - Zusammenfassung der Computer in eine Gruppe, um deren Verwaltung zu erleichtern. Die Gruppe wird als Ganzes verwaltet und kann eine Gruppenrichtlinie haben, andere Gruppen einschließen und Verwaltungsbefehle ausführen.

Virtuelles Laufwerk (RAM-Laufwerk) – Bereich des Arbeitsspeichers (RAM) eines PC, der ein normales physisches Laufwerk simuliert und sich wie dieses verhält.

Vollständige Untersuchung - ein Modus des Anwendungsbetriebs, bei welchem auf Anfrage des Benutzers der ganze Computer auf virenähnliche Codes durchsucht und eventuell erkannte verdächtige bzw. infizierte Objekte gesäubert oder entfernt werden können.

W

Werbe-Programme (*Adware*) – Programmcode, der ohne Kenntnis des Benutzers in einem Programm eingebaut ist, um Werbeanzeigen darzustellen. In der Regel sind Werbeprogramme in Software-Lösungen enthalten, die kostenlos vertrieben werden. Die Werbung wird auf der Arbeitsoberfläche untergebracht. Oft sammeln solche Programme Daten und übermitteln an deren Schöpfer persönlichen Informationen über den Benutzer, ändern verschiedene Browser-Einstellungen (Start- und Suchseiten, Sicherheitsstufen usw.) und erzeugen Datenverkehr, der vom Benutzer nicht zu kontrollieren ist. Alle jene Vorgänge können gegen die Sicherheitsrichtlinie verstoßen und direkte, finanzielle Einbußen bewirken.

Wiederherstellen – Verschieben des Originalobjekts aus der Quarantäne bzw. aus der Backup-Ablage in dessen ursprüngliches Verzeichnis, wo dieses abgelegt war, bevor er in Quarantäne verschoben, gesäubert oder gelöscht wurde.

Z

Zentrale Programmverwaltung – Verwaltung der Anwendung mit Hilfe von Verwaltungsdiensten des Kaspersky Administration Kit 5.0.

Zusätzliche NTFS-Streams (NTFS-Streams) – Datenströme eines Laufwerks mit einem NTFS-Dateisystem, die den Hauptdatenstrom ergänzen, in dem ihr Inhalt abgespeichert ist.

ANHANG C. KASPERSKY LAB

Das Unternehmen

Kaspersky Lab ist ein weltweit führendes Unternehmen in den Bereichen Viren-, Spam- und Hacker-Schutz. Unser hoch spezialisiertes Viren-Labor reagiert stets schneller als alle anderen auf neue Bedrohungen, so dass unsere innovativen Programme seit vielen Jahren Heimanwender und Unternehmen jeder Größe zuverlässig schützen.

Bereits 1997 wurde Kaspersky Lab von dem russischen Virenexperten Eugene Kaspersky in Moskau gegründet und hat heute unter anderem Niederlassungen in Deutschland, Frankreich, Großbritannien, Polen, Japan, USA und China.

Einzigartige Erfahrung

Weltweit beschäftigt Kaspersky Lab über 550 hochspezialisierte Mitarbeiter, darunter Mitglieder der Computer Anti-Virus Researchers Organisation (CARO) und des Virus Bulletin Technical Advisory Board. Im Laufe vieler Jahre Forschung und Kampf gegen Computerviren haben wir Wissen und Fähigkeiten erworben, die heute unser wertvollstes Kapital darstellen.

Dank unserer weit reichenden Erfahrung sind wir in der Lage, Entwicklungstrends bei Malware vorherzusehen. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab, so dass wir anderen immer einen Schritt voraus sind und unseren Kunden stets den besten Schutz bieten können.

Kaspersky Anti-Virus

Nach vielen Jahren innovativer Entwicklungen zählt Kaspersky Lab heute zu den führenden Herstellern von Sicherheits-Software. Der hohe Standard unserer Produkte wird durch zahlreiche Auszeichnungen internationaler Forschungseinrichtungen, unabhängiger Testlabors und renommierter Fachpublikationen bestätigt.

Die Programm-Module unseres bekanntesten Programms, Kaspersky Anti-Virus, gewährleisten einen zuverlässigen Schutz für Workstations, Datei- und Web-Server, Mail-Gateways, Firewalls, Pocket-PCs und Smartphones.

Als erstes Unternehmen entwickelte Kaspersky Lab bedeutende Technologien, die heute selbst bei zahlreichen Antiviren-Programmen anderer Hersteller – wie G-Data, Aladdin und F-Secure – als Programm-Kern einen unverzichtbaren Bestandteil bilden. So vertrauen bereits über 200 Millionen Anwender unseren Innovationen, wie dem heuristischen Analysator zur Entdeckung noch unbekannter Viren, den Micro-Updates für die Antiviren-Datenbanken und dem ersten umfassenden Virenschutz für Unix/Linux-Systeme.

Komplexe Technologien für Ihre Sicherheit

Moderne Viren und Schadprogramme sind komplexe Bedrohungen, so dass die bisher üblichen Schutzpakete für PCs und Netzwerke häufig nicht mehr ausreichen.

Aus diesem Grund entwickelte Kaspersky Lab mit Kaspersky Anti-Hacker eine Personal Firewall und mit Kaspersky Anti-Spam einen besonders effektiven Spam-Filter. Mit den Produkten von Kaspersky Lab können Sie Ihren Computer und Ihr Netzwerk optimal vor allen modernen virtuellen Gefahren schützen.

Service

Kaspersky Lab bietet seinen Kunden eine ganze Palette zusätzlicher Dienstleistungen, die einen maximalen Schutz garantieren: Die Antiviren-Datenbanken werden stündlich aktualisiert, die Anti-Spam-Dateien 12 bis 24 Mal pro Tag. Zudem steht allen Anwendern ein rund-um-die-Uhr-Support zur Verfügung: Telefonisch oder per E-Mail – in deutscher, englischer, russischer und französischer Sprache.

C.1. Andere Produkte von Kaspersky Lab

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus Personal schützt Ihren daheim genutzten Computer unter Microsoft Windows 98/ME, 2000/NT/XP vor allen bekannten Virenarten einschließlich potentiell gefährlicher Software. Das Programm kontrolliert laufend sämtliche Kanäle für möglichen Virenbefall – E-Mail, Internet, Disketten, CDs u.a. Das einmalige heuristische Datenanalyse-System neutralisiert auf wirksame Weise unbekannte Viren. Folgende Varianten für die Arbeit des Programms lassen sich unterscheiden (Diese können separat oder gemeinsam verwendet werden):

- **Echtzeitschutz des Computers** – Virenuntersuchung aller Objekte, die auf dem Computer gestartet, geöffnet und gespeichert werden.
- **Scan auf Befehl** – Untersuchung und Desinfektion sowohl des gesamten Computers als auch einzelner Laufwerke, Dateien oder Verzeichnisse. Sie können diese Untersuchung selbständig starten oder den regelmäßigen automatischen Start der Untersuchung konfigurieren.

Kaspersky Anti-Virus Personal untersucht nun Objekte, die während einer vorhergehenden Untersuchung gescannt wurden und seitdem nicht verändert wurden, nicht erneut. Dies gilt sowohl für den Echtzeitschutz als auch für den Scan auf Befehl. Dadurch **erhöht sich die Operationsgeschwindigkeit des Programms wesentlich**.

Das Programm schafft eine zuverlässige Barriere gegen das Eindringen von Viren über E-Mails. Kaspersky Anti-Virus Personal führt automatisch die Untersuchung und Desinfektion des gesamten nach den Protokollen POP3 und SMTP ein- und ausgehenden E-Mailverkehrs durch und bietet die effiziente Untersuchung von Mail-Datenbanken.

Das Programm unterstützt mehr als siebenhundert Formate für Archive und komprimierte Dateien, überprüft deren Inhalt auf Viren und eliminiert gefährliche Codes aus **ZIP, CAB, RAR, AFJ, LHA** und **ICE**-Archiven.

Die komfortable Bedienung des Programms wird durch die Auswahl zwischen drei voreingestellten Sicherheitsstufen realisiert: **Maximale Sicherheit**, **Empfohlen** und **Maximales Tempo**.

Die Antiviren-Datenbanken werden alle drei Stunden aktualisiert. Die vollständige Übertragung wird auch bei Unterbrechung oder Wechsel der Internetverbindung garantiert.

Kaspersky Anti-Virus® Personal Pro

Dieses Programmpaket wurde speziell entwickelt, um den vollwertigen Antivirenschutz für Heimcomputer unter den Betriebssystemen Microsoft Windows 98/ME, Microsoft Windows 2000/NT, Microsoft Windows XP, sowie mit Microsoft Office Anwendungen der Business-Edition zu gewährleisten. Kaspersky Anti-Virus® Personal Pro verfügt über eine Funktion zum täglichen Download von Updates für Antiviren-Datenbanken und Programmmodule. Das einmalige heuristische System zur Datenanalyse der zweiten Generation erlaubt, unbekannte Viren wirksam zu neutralisieren. Die einfache und praktische Benutzeroberfläche ermöglicht das schnelle Anpassen der Einstellungen und sorgt für größtmöglichen Komfort im Umgang mit dem Programm.

Kaspersky Anti-Virus® Personal Pro bietet:

- **die Antiviren-Untersuchung** der lokalen Laufwerke **auf Befehl des Benutzers**.
- **die automatische Untersuchung im Echtzeitmodus** auf Viren in allen verwendeten Dateien.
- **einen E-Mail-Filter**, der automatisch die Untersuchung und Desinfektion des gesamten nach den Protokollen POP3 und SMTP ein- und ausgehenden E-Mail-Verkehrs vornimmt und Mail-Datenbanken effektiv auf Viren untersucht.
- **Behaviour Blocker**, der hundertprozentigen Schutz vor Makroviren für MS Office Anwendungen garantiert.
- **die Antiviren-Untersuchung** von über 900 Versionen archivierter und gepackter Dateiformate und gewährleistet die automatische Antiviren-Untersuchung des Inhalts, sowie das Entfernen von schädlichem Code aus Archivdateien der Formate **ZIP**, **CAB**, **RAR**, **ARJ**, **LHA** und **ICE**.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker ist eine persönliche Firewall, die Ihren Computer unter Microsoft Windows vollständig gegen unberechtigten Zugriff auf Daten und gegen Hackerangriffe über das Internet oder lokale Netzwerke abschirmt.

Kaspersky® Anti-Hacker verfolgt die Netzaktivitäten über ein TCP/IP-Protokoll für sämtliche Anwendungen auf Ihrem Computer. Falls für eine Anwendung verdächtige Aktivitäten registriert werden, gibt das Programm eine Warnmeldung aus und blockiert, falls erforderlich, den Zugriff über das Netz für die entsprechende Anwendung, so dass die auf dem Computer gespeicherten Daten geschützt bleiben.

Durch Verwendung der SmartStealth™-Technologie wird das Aufspüren des Computers von außerhalb erheblich erschwert: da der Computer unsichtbar bleibt, ist er vor Hackerangriffen geschützt, ohne dass jedoch Ihre eigene Kommunikations- und Arbeitsfähigkeit über das Internet beeinträchtigt wird. Das Programm gewährleistet angemessenen Schutz aber auch den standardmäßigen Zugriff auf die Daten des Computers.

Kaspersky® Anti-Hacker blockiert weiterhin die am weitesten verbreiteten Formen von Netzattacken durch Hacker sowie Versuche zum Ausspähen einzelner Ports.

Das Programm bietet vereinfachte Steuerungsmöglichkeiten über fünf verschiedene Sicherheitsstufen. Als Standardeinstellung wird eine lernfähige Systemkonfiguration verwendet, so dass die Sicherheitseinstellungen an Ihre individuelle Reaktion auf verschiedene Ereignisse angepasst werden können. Dadurch wird es möglich, die Konfiguration der Firewall individuell auf bestimmte Anwender und einzelne Computer abzustimmen.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite ist ein Programmkomplex, welcher der Organisation des umfassendes Schutzes eines PCs unter dem Betriebssystem Microsoft Windows dient. Der Komplex verhindert das Eindringen von schädlichen und potentiell gefährlichen Programmen über alle möglichen Quellen, gewährleistet den Schutz vor Versuchen zum unerlaubten Zugrifff auf Daten des Computers und schützt vor Spam.

Kaspersky® Personal Security Suite verfügt über folgende Funktionen:

- Antivirenschutz der Daten, die auf dem Computer gespeichert sind.
- Schutz der Benutzer der Mail-Clients Microsoft Office Outlook und Microsoft Outlook Express vor unerwünschten E-Mails (Spam).
- Schutz des Computers vor unerlaubtem Datenzugriff sowie Schutz vor Netzwerkangriffen aus dem lokalen Netzwerk oder Internet.

Kaspersky Lab News Agent

Das Programm News Agent dient der schnellen Zustellung der Nachrichten von Kaspersky Lab, der Benachrichtigung über das "Virus-Wetter" und über neu erschienene Nachrichten. Das Programm liest in vorgegebenen Zeitabständen von den Kaspersky-Lab-Newsservern eine Liste der verfügbaren Nachrichtenkanäle und der darin enthaltenen Informationen.

News Agent verfügt außerdem über folgende Funktionen:

- Visualisierung des Zustands des "Viren-Wetters" im Infobereich der Taskleiste.
- Abonnieren und Abbestellen der Nachrichtenkanäle von Kaspersky Lab.
- Download von Nachrichten für jeden abonnierten Kanal in festgelegten Zeitabständen. Außerdem erfolgt eine Benachrichtigung über ungelesene Nachrichten.
- Anzeige von Nachrichten der abonnierten Kanäle.
- Anzeige einer Liste der Kanäle und ihrer Status.
- Öffnen der Webseite mit dem vollständigen Nachrichtentext im Browser.

News Agent funktioniert unter dem Betriebssystem Microsoft Windows. Er kann als separates Produkt benutzt werden oder zu unterschiedlichen integrierten Lösungen von Kaspersky Lab gehören.

Kaspersky OnLine Scanner

Dieses Programm ist ein kostenloser Dienst, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antivirenuntersuchung des Computers im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Webbrowser ausgeführt und verwendet die Technologie Microsoft ActiveX®. Dadurch kann der Benutzer auf schnelle Weise herausfinden, ob sein Computer von einer Infektion durch schädliche Programme bedroht ist. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Antiviren-Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

Kaspersky® OnLine Scanner Pro

Dieses Programm stellt einen Abonnementsdienst dar, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antivirenuntersuchung des Computers und die Desinfektion infizierter Dateien im Online-Modus erlaubt. Kaspersky OnLine Scanner Pro wird direkt im Webbrowser ausgeführt und

verwendet die Technologie Microsoft ActiveX®. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Antiviren-Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 dient dem Schutz eines Personalcomputers vor schädlichen Programmen. Dabei werden traditionelle Virenschutzmethoden auf optimale Weise mit neuen proaktiven Technologien vereinigt.

Das Programm erlaubt eine komplexe Antivirenuntersuchung, die folgende Optionen umfasst:

- Antivirenuntersuchung des Mail-Datenstroms auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm, sowie Untersuchung und Desinfektion von Mail-Datenbanken.
- Antivirenuntersuchung des Internet-Datenstroms, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- Antivirenuntersuchung beliebiger einzelner Dateien, Ordner und Laufwerke. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystem Microsoft Windows gestartet werden, vorhanden.

Der Proaktive Schutz umfasst:

- **Kontrolle über Veränderungen im Dateisystem**. Das Programm erlaubt es, eine Liste der Anwendungen anzulegen, deren Komponentenbestand kontrolliert werden soll. Dadurch lässt sich die Verletzung der Integrität von Anwendungen durch Schadprogramme verhindern.
- **Überwachung von Prozessen im Arbeitsspeicher**. Kaspersky Anti-Virus 6.0 warnt den Benutzer rechtzeitig, wenn gefährliche, verdächtige oder versteckte Prozesse auftreten oder wenn normale Prozesse auf unerlaubte Weise verändert werden.
- **Überwachung von Veränderungen in der Registrierung des Betriebssystems** durch die Kontrolle des Zustands der Systemregistrierung.
- **Sperren gefährlicher Makros** des Typs Visual Basic for Applications in Microsoft Office Dokumenten.

- **Systemwiederherstellung** nach schädlicher Einwirkung von Spyware: Die Wiederherstellung wird durch die Speicherung aller Veränderungen in der Registrierung und im Dateisystem des Computers und durch das vom Benutzer initiierte Rückgängigmachen der Veränderungen ermöglicht.

Kaspersky® Internet Security 6.0

Kaspersky® Internet Security 6.0 ist eine komplexe Lösung für den Schutz eines Personalcomputers vor den wichtigsten Bedrohungen (Viren, Hackerangriffe, Spam und Spyware), denen Informationen unterliegen. Alle Komponenten lassen sich über eine einheitliche Benutzeroberfläche einstellen und steuern.

Die Funktion des Antivirenschutzes umfasst:

- **Antivirenuntersuchung des Mail-Datenstroms** auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm. Für die populären Mailprogramme Microsoft Office Outlook, Microsoft Outlook Express und The Bat! sind Plugins und die Desinfektion von Mail-Datenbanken vorgesehen.
- **Antivirenuntersuchung des Internet-Datenstroms**, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- **Schutz des Dateisystems**: Der Antivirenuntersuchung können beliebige einzelne Dateien, Ordner und Laufwerke unterzogen werden. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystem Microsoft Windows gestartet werden, vorhanden.
- **Proaktiver Schutz**: Das Programm führt die ununterbrochene Überwachung der Aktivität von Anwendungen und Prozessen durch, die im Arbeitsspeicher des Computers gestartet werden, verhindert gefährliche Veränderungen des Dateisystems und der Registrierung, und stellt das System nach schädlicher Einwirkung wieder her.

Der **Schutz vor Internetbetrug** beruht auf dem Erkennen von Phishing-Angriffen. Dadurch lässt sich der Diebstahl Ihrer vertraulichen Informationen verhindern (in erster Linie Kennwörter, Konto- und Kreditkartennummern, sowie Sperren der Ausführung gefährlicher Skripts auf Webseiten, Sperren von Popupfenstern und Werbebannern). Die Funktion zum **Sperren der Einwahl auf kostenpflichtige Telefonnummern** ermöglicht es, Programme zu identifizieren, die versuchen Ihr Modem für versteckte Verbindungen mit kostenpflichtigen Telefondiensten zu missbrauchen, indem diese Programme gesperrt werden.

Kaspersky® Internet Security 6.0 **erkennt Versuche zum Scannen der Ports Ihres Computers**, die häufig Netzwerkangriffe ankündigen. Auf der **Basis von vordefinierten Regeln** führt das Programm die Kontrolle aller Netzwerkaktionen durch und überwacht alle **eingehenden und ausgehenden Datenpakete**. Der

Stealth-Modus (SmartStealth™-Technologie) **macht den Computer für die externe Umgebung praktisch unsichtbar**. In diesem Modus wird jede Netzwerkaktivität verboten, wenn sie nicht durch Ausnahmeregeln erlaubt wird, die vom Benutzer festgelegt wurden.

Im Programm wird ein komplexe Methode zur Spam-Filterung eingehender Mails angewandt:

- Untersuchung nach schwarzen und weißen Adressenlisten (einschließlich Adressen von Phishing-Seiten)
- Phrasenuntersuchung im Mail-Text
- Analyse des Mail-Texts mit Hilfe eines lernfähigen Algorithmus
- Erkennung von Spam in Form von Grafiken

Kaspersky® Security für PDA

Kaspersky® Security für PDA gewährleistet zuverlässigen Virenschutz für Daten auf Handheld-PCs unter Palm OS oder Microsoft Windows CE sowie für Daten, die von einem gewöhnlichen PC oder Erweiterungsspeichern, von CD-ROM oder aus Datenbanken übernommen werden. Das Programm umfasst eine optimale Auswahl an Virenschutz-Komponenten:

- **einen Virenscanner**, der eine Überprüfung der Daten (sowohl im Speicher des PDA selbst, als auch auf beliebigen Speicher-Erweiterungskarten) auf Anforderung des Anwenders ausführt;
- **den Antivirus-Monitor**, der während der Synchronisation über HotSync™ und während des Datenaustausches mit anderen PDA Virenprogramme blockiert.

Weiterhin schützt das Programm die auf dem PDA gespeicherten Informationen vor unberechtigtem Zugriff durch Verschlüsselung des Zugriffs auf das Gerät selbst wie auch auf die im Speicher des PDA und auf Speicherkarten enthaltenen Daten.

Kaspersky Anti-Virus® Business Optimal

Dieses Programmpaket ist die ultimative Lösung zum Schutz vor Computerviren für Unternehmen kleiner und mittlerer Größe.

Kaspersky Anti-Virus® Business Optimal bietet Rundumschutz[9] vor Viren für:

- *Computerarbeitsplätze* unter Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation, Linux.
- *Dateiserver* unter Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD und OpenBSD, Linux, Samba Servers.
- *Mailsysteme* vom Typ Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail und Qmail.
- *Internet-Firewalls*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

Kaspersky Anti-Virus® Business Optimal beinhaltet außerdem das zentrale Installations- und Administrationssystem Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

Kaspersky® Corporate Suite

Kaspersky® Corporate Suite ist eine integrierte Softwarelösung zum Datenschutz für Ihr gesamtes Firmennetzwerk ohne Einschränkungen hinsichtlich Größe und Struktur. Die enthaltenen Programmkomponenten schützen jeden Punkt ihres firmeninternen Netzes. Sie sind kompatibel mit den meisten heute verbreiteten Betriebssystemen und Anwendungen, über ein zentrales Steuerungssystem miteinander verbunden und werden über eine gemeinsame Benutzeroberfläche bedient. Mit diesem System erhalten Sie einen Virenschutz, der sich vollständig an die Systemanforderungen Ihres internen Netzes anpassen lässt.

Kaspersky® Corporate Suite bietet Rundumschutz[10] vor Viren für:

- *Computerarbeitsplätze* unter Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation und Linux.
- *Dateiserver* unter Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux und Samba Servers.
- *Mailsysteme* vom Typ Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim und Qmail.
- *Internet-Firewalls*: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition.

---

[9] Je nach Lieferumfang
[10] Je nach Lieferumfang

- Handheld-PCs, die unter Microsoft Windows CE und Palm OS arbeiten, sowie Smartphones, die unter Microsoft Windows Mobile 2003 for Smartphone und Microsoft Smartphone 2002 arbeiten.

Kaspersky® Corporate Suite beinhaltet außerdem das zentrale Installations- und Administrationssystem Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam ist die erste in Russland entwickelte Software zum Schutz vor unerwünschten Mailings (Spam) für Unternehmen kleinerer und mittlerer Größe. Das Programm vereint moderne Verfahren der Sprachanalyse für Informationen in Textform, sämtliche modernen Verfahren zum Filtern von E-Mails (einschließlich RBL-Listen und formeller Prüfung von Nachrichten) sowie eine einmalige Auswahl an Dienstprogrammen, durch die der Nutzer in die Lage versetzt wird, bis zu 95 % der unerwünschten Nachrichten zu identifizieren und zu eliminieren.

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am „Eingang“ des firmeninternen Netzwerks installiert, sämtliche eingehenden Mitteilungen auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

Die tägliche Aktualisierung der Filterdatenbank mit Mustertexten aus unserem Sprachlabor garantiert eine hohe Effizienz dieses Produkts. Die Datenbank-Updates erscheinen alle 20 Minuten.

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux / Unix dient der Antivirenbearbeitung von E-Mails, die mit SMTP-Protokoll weitergeleitet werden. Die Anwendung umfasst eine Reihe von zusätzlichen Filterinstrumenten für den Mailverkehr (Filterung nach Namen und MIME-Typen von Attachments) sowie eine Reihe von Mitteln, die es erlauben, die Belastung des Mailsystems zu verringern und Hackerangriffe abzuwehren. Dazu zählen die Begrenzung der maximalen Mailgröße, der Anzahl von Adressaten usw. Die Unterstützung der Technologie DNS Black List schützt vor dem Empfang von Mails, die von Servern stammen, die auf diesen Listen stehen und als Verbreitungsquellen für Spam gelten.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security® for Microsoft Exchange bietet die Antivirenuntersuchung der eingehenden, ausgehenden und auf dem Server gespeicherten E-Mail-Nachrichten einschließlich der Nachrichten in gemeinsamen Ordnern. Außerdem führt er die Filterung unerwünschter Korrespondenz aus, wobei intelligente Technologien zur Spam-Erkennung in Verbindung mit Technologien der Firma

Microsoft verwendet werden. Die Anwendung untersucht alle mit dem SMTP-Protokoll auf dem Exchange-Server eingehenden Nachrichten auf das Vorhandensein von Viren, wobei Antivirentechnologien von Kaspersky Lab verwendet werden, und auf Spam-Merkmale, wozu die Filterung nach formalen Kennzeichen (E-Mail-Adresse, IP-Adresse, Größe der Mail, Kopfzeile) dient. Außerdem analysiert er den Inhalt des Briefs und seiner Anhänge mit Hilfe von intelligenten Technologien, die unikale grafische Signaturen zum Erkennen von Spam in grafischer Form umfassen. Der Untersuchung werden sowohl der Nachrichtenkörper als auch angehängte Dateien unterzogen.

Kaspersky® Mail Gateway

Kaspersky® Mail Gateway ist eine universelle Lösung für den komplexen Schutz der Benutzer von Mailsystemen. Die Anwendung wird zwischen dem Unternehmensnetzwerk und dem Internet installiert und führt die Untersuchung aller Elemente einer E-Mail auf das Vorhandensein von Viren und anderen schädlichen Programmen (Spyware, Adware usw.) durch. Außerdem erfolgt die zentralisierte Filterung des E-Mail-Nachrichtenstroms auf Spam-Merkmale. Die Lösung enthält ferner eine Reihe zusätzlicher Optionen für die Filterung des E-Mail-Stroms.

C.2. Kontaktinformationen

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gern umfassend per Telefon oder E-Mail beraten.

Weitere Information erhalten Sie bei:

Kaspersky Labs GmbH

Steinheilstraße 13

85053 Ingolstadt

Technischer Support	Tel.: +49 (0) 841 98 18 90 Fax: +49 (0) 841 98 18 918 E-Mail: info@kaspersky.de
Allgemeine Informationen	WWW: http://www.kaspersky.com/de/ http://www.viruslist.com/de/

Feedback zu unseren Benutzerhand-büchern	docfeedback@kaspersky.com (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

ANHANG D. ENDBENUTZER-LIZENZVERTRAG

WICHTIG - bitte sorgfältig lesen: Lesen Sie die in diesem Kaspersky Lab Endbenutzer-Lizenzvertrag ("EULA") beschriebenen Rechte und Einschränkungen sorgfältig durch. Sie werden gebeten, die Bestimmungen des EULAs zu prüfen und ihnen zuzustimmen oder diese abzulehnen.

Wenn Sie die SOFTWARE installieren, erklären Sie sich mit den Bestimmungen des EULAs einverstanden. Falls Sie mit den Bestimmungen des EULAs NICHT einverstanden sind, geben Sie die erworbene Software bitte innerhalb von 30 Tagen an die Einkaufsstelle zurück.

Jede Bezugnahme auf "Software" schließt den Software-Aktivierungsschlüssel ("Key Identification File" [Schlüssel-Identifikationsdatei]) ein, den Sie von Kaspersky Lab als Teil der Software erhalten.

Dieser EULA ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Besitzer eines Exemplars der Kaspersky SOFTWARE (entweder als natürlicher oder als juristischer Person) und Kaspersky Lab. Kaspersky Lab wird sich das exklusive Urheberrecht auf die Computersoftware (auf die Software und die Antiviren-Datenbanken) vorbehalten. Indem Sie die SOFTWARE installieren, erklären Sie sich damit einverstanden, durch die Bestimmungen dieses EULAs gebunden zu sein. Falls Sie den Bestimmungen dieses EULAs nicht zustimmen, sind Sie nicht berechtigt, die SOFTWARE zu installieren und zu verwenden.

Die SOFTWARE ist sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum geschützt. Die SOFTWARE wird lizenziert, nicht verkauft.

1. LIZENZEINRÄUMUNG. Durch diesen EULA werden Ihnen folgende Rechte eingeräumt:

- Sie sind berechtigt, eine Kopie der SOFTWARE auf einem einzigen Computer zu installieren und zu verwenden.
- Sie sind berechtigt, die installierte SOFTWARE für die Dauer (Lizenzdauer) zu benutzen, die in der Schlüsseldatei (die unikale Datei, die erforderlich ist, um die Software vollständig zu aktivieren. Bitte beachten Sie Hilfe/Über das Programm, für die Unix/Linux-Version der Software siehe Bemerkung über die Gültigkeitsdauer der Schlüsseldatei) angegeben ist, außer wenn der Vertrag früher als hierdurch vorgesehen gekündigt wird. Sie können diesen Vertrag jederzeit kündigen, indem Sie alle Kopien der Software und der Dokumentation zerstören.

2. EINSCHRÄNKUNGEN

- Einschränkungen im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, die SOFTWARE zurückzuentwickeln (Reverse Engineering), zu dekompilieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet. Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.
- Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.
- Supportleistungen. Nach Kauf der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die Lizenzdauer. Supportleistungen verstehen sich wie folgt:
    - stündliches Update der Antiviren-Datenbank
    - kostenloses Update der Software
    - kostenlose technische Unterstützung sowohl per E-Mail als auch per Telefon mit Hot-Line-Service
- Viren-Entdeckung und heilende Updates auf Anfrage innerhalb von 48 Stunden.

3. KÜNDIGUNG. Unbeschadet sonstiger Rechte ist Kaspersky Lab berechtigt, diesen EULA zu kündigen, sofern Sie gegen die Bestimmungen dieses EULAs verstoßen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien der SOFTWARE und alle ihre Komponenten zu vernichten.

4. URHEBERRECHT. Eigentum und Urheberrecht auf die SOFTWARE, die gedruckten Begleitmaterialien und jede Kopie der SOFTWARE liegen bei Kaspersky Lab.

5. GEWÄHRLEISTUNG. KASPERSKY LAB gewährleistet, dass:

- die SOFTWARE den Spezifikationen im wesentlichen entspricht.
- der Originaldatenträger frei von Material- und Herstellungsfehlern ist.
- das Programm korrekt auf dem Datenträger aufgezeichnet ist, die Dokumentation sämtliche Informationen enthält, die KASPERSKY LAB für die Benutzung der Software für erforderlich hält.
- die SOFTWARE binnen 6 Monaten ab der ersten Installation oder dem ersten Download, falls richtig behandelt, vollfunktionsfähig ist, der in der beiliegenden Dokumentation bestimmten Funktionalität entsprechend.

Die Gewährleistungsfrist beträgt 6 Monate ab der ersten Installation oder dem ersten Download der Software den beiliegenden Dokumentationen von Kaspersky Lab entsprechend. Gewährleistungspflichtige Mängel werden von KASPERSKY LAB oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der Gewährleistungsfrist, dem Ermessen von Kaspersky Lab nach, durch Ersatz, Reparatur, Umtausch oder Rückzahlung beseitigt, falls eine Mängelrüge rechtzeitig an Kaspersky Lab oder dessen Lieferanten gerichtet wurde. KASPERSKY LAB oder dessen Lieferanten übernehmen keine Gewährleistung für Mängel, die auf andere als für die Software vorgesehenen Einsatzbedingungen, unsachgemäße Behandlung oder dergleichen zurückzuführen sind.

ALLE ANDERE GEWÄHRLEISTUNGEN UND BEDINGUNGEN, SEIEN SIE AUSDRÜCKLICH ODER KONKLUDENT, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF, (FALLS ZUTREFFEND) JEDE KONKLUDENTE GEWÄHRLEISTUNG IM HINBLICK AUF HANDELSÜBLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, FAHRLÄSSIGKEIT ODER MANGELNDE FACHMÄNNISCHE BEMÜHUNGEN WERDEN VON KASPERSKY LAB ODER DESSEN LIEFERANTEN ABGELEHNT. ES BESTEHT EBENFALLS KEINE GEWÄHRLEISTUNG ODER BEDINGUNG VON RECHTSANSPRÜCHEN IN BEZUG AUF RECHTSINHABERSCHAFT, UNGESTÖRTES NUTZUNGSVERGNÜGEN ODER NICHTVERLETZUNG VON RECHTEN DRITTER. DAS GESAMTE RISIKO, DAS BEI DER BENUTZUNG ODER LEISTUNG DER SOFTWARE ENTSTEHT, LIEGT BEI IHNEN.

6. AUSSCHLUSS DER HAFTUNG FÜR ALLE SCHÄDEN. SOWEIT GESETZLICH ZUGELASSEN, SIND KASPERSKY LAB ODER DESSEN LIEFERANTEN IN KEINEM FALL HAFTBAR FÜR IRGENDWELCHE FOLGE-, ZUFÄLLIGEN, DIREKTEN, INDIREKTEN, SPEZIELLEN, STRAFRECHTLICHEN ODER ANDEREN SCHÄDEN WELCHER ART AUCH IMMER (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AN PERSONEN ODER SACHEN, SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG, VERLUST VON GESCHÄFTLICHEN INFORMATIONEN, FÜR DEN VERLUST VON PRIVATSPHÄRE, DIE UNMÖGLICHKEIT, EINE PFLICHT ZU ERFÜLLEN (EINSCHLIESSLICH GEMÄSS TREU UND GUTEN GLAUBENS ODER VERNÜNFTIGER ANGEMESSENER SORGFALT) ZU ERFÜLLEN, FÜR FAHRLÄSSIGKEIT ODER ANDERE VERMÖGENSSCHÄDEN), DIE AUS DER VERWENDUNG DER SOFTWARE ODER DER TATSACHE, DASS SIE NICHT VERWENDET WERDEN KANN, RESULTIEREN ODER DAMIT IN ZUSAMMENHANG STEHEN, SELBST WENN KASPERSKY LAB ODER DESSEN LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WORDEN IST. DIESER HAFTUNGSAUSSCHLUSS FÜR SCHÄDEN GILT AUCH DANN, WENN ABHILFEMASSNAHMEN IHREN WESENTLICHEN ZWECK VERFEHLEN.

7. ANWENDBARES RECHT. Dieser Vertrag unterliegt der Gesetzgebung der Bundesrepublik Deutschland.